Cryptographic Protocols (2DMI00)
Exam, July 5, 2023, 18:00–21:00h

Solve the following four problems, providing full motivation for the correctness of your solutions.

No calculators or any other electronic devices are allowed, nor any notes or books.

Please, hand in your answer pages, not your scratch paper.

1. Let $\langle g \rangle$ be a cyclic group of order n.

Let distributions X, Y, Z be given by:

$$\begin{aligned} X &= \{(g^x, g^y) : x, y \in_R \mathbb{Z}_n\}, \\ Y &= \{(g^x, g^y) : x \in_R \mathbb{Z}_n, y \in_R \mathbb{Z}_n^*\}, \\ Z &= \{(g^x, g^y) : x \in_R \mathbb{Z}_n^*, y \in_R \mathbb{Z}_n\}. \end{aligned}$$

Let Δ denote statistical distance.

a) *Assume n is prime. Determine $\Delta(X;Y)$, $\Delta(X;Z)$, and $\Delta(Y;Z)$.*

b) *Determine $\Delta(X;Y)$, $\Delta(X;Z)$, and $\Delta(Y;Z)$ for any n, $n \geq 2$.*

2. Let $\langle g \rangle$ be a cyclic group of order n.

Show that each of the following computational problems is random self-reducible.

a) *Given g^x, g^y, compute $g^{x^2+y^2}$, where $x, y \in \mathbb{Z}_n$.*

b) *Given g^x, g^y, compute $g^{x^2+y^2}$, where $x \in \mathbb{Z}_n^*$ and $y \in \mathbb{Z}_n$.*

3. Let $\langle g \rangle$ be a cyclic group of large prime order n. Let $h \in \langle g \rangle$ denote a random group element such that $\log_g h$ is unknown to anyone.

Consider relation R:

$$R = \{(A, B, C; x, y) : A = g^x \ \wedge \ B = h^y \wedge \ (C = g^{x^2} h^y \ \vee \ C = g^x h^{y^2})\}.$$

a) *Give a Σ-protocol for relation R and prove that it is complete, special sound, and special honest-verifier zero-knowledge.*

b) *Let H be a cryptographic hash function. Turn your Σ-protocol into a noninteractive Σ-proof (using the Fiat-Shamir heuristic) and show how the Σ-proof is verified.*

4. Recall the general shape of a Σ-protocol for a relation R:

Prover $\mathcal{P}$		Verifier $\mathcal{V}$
$((v; w) \in R)$		$(v \in V)$
$a \leftarrow \alpha(v; w; u_{\mathcal{P}})$		
	$\xrightarrow{\text{announcement } a}$	
		$c \in_R C$
	$\xleftarrow{\text{challenge } c}$	
$r \leftarrow \rho(v; w; c; u_{\mathcal{P}})$		
	$\xrightarrow{\text{response } r}$	
		$\varphi(v; a; c; r)?$

Let S denote a simulator for the Σ-protocol.

Let $v \in L_R$ be given.

Consider the following commitment scheme for a sender and a receiver.

Commit Phase. The sender commits to value $c \in C$ by running $(a; c; r) \leftarrow S(v; c)$ and sending commitment a to the receiver.

Reveal Phase. The sender opens commitment a by sending c and r to the receiver. The receiver checks if $\varphi(v; a; c; r)$ holds for the already received commitment a.

a) *Instantiate the commitment scheme using Schnorr's Σ-protocol for relation $R = \{(h; x) : h = g^x\}$ and show how this corresponds to Pedersen's commitment scheme.*

Next, show that the commitment scheme works in general for an arbitrary nontrivial Σ-protocol (that is, for any protocol of the above shape with $|C| \geq 2$ satisfying completeness, special soundness, and special honest-verifier zero-knowledgeness), assuming it is hard to find any witness w such that $(v; w) \in R$.

b) *Show that the receiver's check succeeds if both parties follow the protocol steps.*

c) *Show that the commitment scheme is computationally binding*

d) *Show that the commitment scheme is information-theoretically hiding.*

1a:	6	2a:	6	3a:	11	4a:	2	4c:	4
1b:	6	2b:	6	3b:	3	4b:	2	4d:	4

The final mark is the total number of points divided by 5, rounded to one decimal place.

Cryptographic Protocols (2DMI00)
Exam, April 19, 2023, 13:30–16:30h

Solve the following four problems, providing full motivation for the correctness of your solutions.

No calculators or any other electronic devices are allowed, nor any notes or books.

Please, hand in your answer pages, not your scratch paper.

1. Let $\langle g \rangle$ be a cyclic group of order n.

Let distributions X, Y, Z be given by:

$$\begin{aligned} X &= \{(g^x, g^y, g^{x/y}) : x \in_R \mathbb{Z}_n, y \in_R \mathbb{Z}_n^*\}, \\ Y &= \{(g^x, g^y, g^z) : x, z \in_R \mathbb{Z}_n, y \in_R \mathbb{Z}_n^*, z - x/y \in \mathbb{Z}_n^*\}, \\ Z &= \{(g^x, g^y, g^z) : x, z \in_R \mathbb{Z}_n, y \in_R \mathbb{Z}_n^*\}. \end{aligned}$$

Let Δ denote statistical distance.

a) *Assume n is prime. Determine $\Delta(X;Y)$, $\Delta(X;Z)$, and $\Delta(Y;Z)$.*

b) *Determine $\Delta(X;Y)$, $\Delta(X;Z)$, and $\Delta(Y;Z)$ for any n, $n \geq 2$.*

2. Let $\langle g \rangle$ be a cyclic group of order n.

Show that each of the following computational problems is random self-reducible.

a) *Given g^x, g^y, g^z, compute $g^{x^2(y/z)^2}$, where $x, y, z \in \mathbb{Z}_n^*$.*

b) *Given g^x, g^y, g^z, compute $g^{x^2+(y-z)^2}$, where $x, y, z \in \mathbb{Z}_n$ and $y - z \in \mathbb{Z}_n^*$.*

3. Let $\langle g \rangle$ be a cyclic group of large prime order n. Let $h \in \langle g \rangle$ denote a random group element such that $\log_g h$ is unknown to anyone.

Consider relation R:

$$R = \{(A, B; x, y) : A = g^x \ \wedge \ (B = g^{1/x} h^y \vee \ B = g^y h^{1/x}) \wedge \ x \neq 0\}.$$

a) *Give a Σ-protocol for relation R and prove that it is complete, special sound, and special honest-verifier zero-knowledge.*

b) *Let H be a cryptographic hash function. Turn your Σ-protocol into a noninteractive Σ-proof (using the Fiat-Shamir heuristic) and show how the Σ-proof is verified.*

4. Recall the general shape of a Σ-protocol for a relation R:

Prover $\mathcal{P}$		Verifier $\mathcal{V}$
$((v; w) \in R)$		$(v \in V)$
$a \leftarrow \alpha(v; w; u_{\mathcal{P}})$		
	$\xrightarrow{\text{announcement } a}$	
		$c \in_R C$
	$\xleftarrow{\text{challenge } c}$	
$r \leftarrow \rho(v; w; c; u_{\mathcal{P}})$		
	$\xrightarrow{\text{response } r}$	
		$\varphi(v; a; c; r)?$

Let S denote a simulator for the Σ-protocol.

Let $v \in L_R$ be given.

Consider the following commitment scheme for a sender and a receiver.

Commit Phase. The sender commits to value $c \in C$ by running $(a; c; r) \leftarrow S(v; c)$ and sending commitment a to the receiver.

Reveal Phase. The sender opens commitment a by sending c and r to the receiver. The receiver checks if $\varphi(v; a; c; r)$ holds for the already received commitment a.

a) *Instantiate the commitment scheme using Schnorr's Σ-protocol for relation $R = \{(h; x) : h = g^x\}$ and show how this corresponds to Pedersen's commitment scheme.*

Next, show that the commitment scheme works in general for an arbitrary nontrivial Σ-protocol (that is, for any protocol of the above shape with $|C| \geq 2$ satisfying completeness, special soundness, and special honest-verifier zero-knowledgeness), assuming it is hard to find any witness w such that $(v; w) \in R$.

b) *Show that the receiver's check succeeds if both parties follow the protocol steps.*

c) *Show that the commitment scheme is computationally binding*

d) *Show that the commitment scheme is information-theoretically hiding.*

1a:	6	2a:	6	3a:	11	4a:	2	4c:	4
1b:	6	2b:	6	3b:	3	4b:	2	4d:	4

The final mark is the total number of points divided by 5, rounded to one decimal place.

Cryptographic Protocols (2DMI00)
Exam, July 6, 2022, 18:00–21:00h

Solve the following four problems, providing full motivation for the correctness of your solutions.

No calculators or any other electronic devices are allowed, nor any notes or books.

Please, hand in your answer pages, not your scratch paper.

1) For $1 \leq d < n$, consider distributions X, Y, Z given by:

$$\begin{aligned} X &= \{u : u \in_R \{1, \ldots, dn\}\}, \\ Y &= \{un : u \in_R \{1, \ldots, d\}\}, \\ Z &= \{ud : u \in_R \{1, \ldots, n\}\}. \end{aligned}$$

Let Δ denote statistical distance.

a) *Determine* $\Delta(X; Y)$ *and* $\Delta(X; Z)$.

b) *Determine* $\Delta(Y; Z)$ *assuming that also* $\gcd(d, n) = 1$.

c) *Determine* $\Delta(Y; Z)$ *for arbitrary* d, n *with* $1 \leq d < n$.

2. Let $\langle g \rangle$ be a cyclic group of order n.

Show that each of the following computational problems is random self-reducible.

a) *Given* g^x, g^y, g^{xy^2}, *compute* $g^{x^2y^4}$, *where* $x, y \in \mathbb{Z}_n^*$.

b) *Given* $g^x, g^{1/y^2}, g^{xy^2}$, *compute* $g^{x^2y^4}$, *where* $x \in \mathbb{Z}_n$ *and* $y \in \mathbb{Z}_n^*$.

3. Let $\langle g \rangle$ be a cyclic group of large prime order n. Let $h \in \langle g \rangle$ denote a random group element such that $\log_g h$ is unknown to anyone.

Consider relation R:

$$R = \{(A, B, C; x, y) : A = g^x \ \wedge \ B = h^y \wedge \ (C = g^{x^2+y} \vee \ C = h^{x+y^2})\}.$$

a) *Give a* Σ*-protocol for relation* R *and prove that it is complete, special sound, and special honest-verifier zero-knowledge.*

b) *Let* H *be a cryptographic hash function. Turn your* Σ*-protocol into a noninteractive* Σ*-proof (using the Fiat-Shamir heuristic) and show how the* Σ*-proof is verified.*

4. Let $V = \{1, ..., n\}$ with $n \geq 1$.

Let S_n denote the set of permutations on V. Recall that for permutations $\pi, \pi' \in S_n$, their composition $\pi'' = \pi' \circ \pi$ satisfies $\pi''(x) = \pi'(\pi(x))$ for all $x \in V$. Also, for $\pi \in S_n$, its inverse π^{-1} satisfies $\pi^{-1}(\pi(x)) = \pi(\pi^{-1}(x)) = x$ for all $x \in V$.

Consider directed graphs $G = (V, E)$ all with the same vertex set $V = \{1, \ldots, n\}$ but arbitrary edge sets $E \subseteq V \times V$.

Two graphs $G_0 = (V, E_0)$ and $G_1 = (V, E_1)$ are **isomorphic** if there exists a permutation $\pi : V \to V$ such that $(x, y) \in E_0 \Leftrightarrow (\pi(x), \pi(y)) \in E_1$ holds for all $x, y \in V$. We write $G_1 = \pi(G_0)$ and also $G_0 = \pi^{-1}(G_1)$.

Computing such a permutation π given G_0 and G_1 is conjectured to be a hard problem (not in **BPP**).

Consider the following protocol for relation $\{(G_0, G_1; \pi) : G_1 = \pi(G_0)\}$, which proves that G_0 and G_1 are isomorphic and that the prover knows a permutation $\pi \in S_n$ mapping G_0 to G_1:

Prover		Verifier
$\upsilon \in_R S_n$ $H \leftarrow \upsilon(G_0)$		
	$\xrightarrow{H}$	
		$c \in_R \{0, 1\}$
	$\xleftarrow{c}$	
$\rho \leftarrow \begin{cases} \upsilon, & \text{if } c = 0 \\ \upsilon \circ \pi^{-1}, & \text{if } c = 1 \end{cases}$		
	$\xrightarrow{\rho}$	
		$\rho(G_c) \stackrel{?}{=} H$

Show that the protocol is a Σ-protocol:

a) *Show that the protocol is complete.*

b) *Show that the protocol is special sound.*

c) *Show that the protocol is special honest-verifier zero-knowledge.*

1a: 4	1c: 4	2a: 6	3a: 12	4a: 2	4c: 4
1b: 4		2b: 6	3b: 3	4b: 5	

The final mark is the total number of points divided by 5, rounded to one decimal place.

Cryptographic Protocols (2DMI00)
Exam, April 21, 2022, 13:30–16:30h

Solve the following four problems, providing full motivation for the correctness of your solutions.

No calculators or any other electronic devices are allowed, nor any notes or books.

Please, hand in your answer pages, not your scratch paper.

1.) Let $\langle g \rangle$ be a cyclic group of order n, where n is prime. Let $g_1, g_2, h_1, h_2 \in \langle g \rangle^*$.
For fixed $c \in \mathbb{Z}_n^*$, consider distributions R, S given by:

$$\begin{aligned} R_1 &= \{(a_1, a_2; c; r) : u \in_R \mathbb{Z}_n; a_1 \leftarrow g_1^u; a_2 \leftarrow g_2^u; r \leftarrow_n u + cx_1\}, \\ R_2 &= \{(a_1, a_2; c; r) : u \in_R \mathbb{Z}_n; a_1 \leftarrow g_1^u; a_2 \leftarrow g_2^u; r \leftarrow_n u + cx_2\}, \\ S &= \{(a_1, a_2; c; r) : r \in_R \mathbb{Z}_n; a_1 \leftarrow g_1^r h_1^{-c}; a_2 \leftarrow g_2^r h_2^{-c}\}. \end{aligned}$$

Let Δ denote statistical distance.

a) *Determine* $\Delta(R_1; S)$ *if* $\log_{g_1} h_1 = \log_{g_2} h_2$.

b) *Determine* $\Delta(R_1; S)$ *if* $\log_{g_1} h_1 \neq \log_{g_2} h_2$.

Next, assume $\log_{g_1} h_1 = \log_{g_2} h_2$. For fixed $c \in \mathbb{Z}_n^*$, consider also distributions R', S' given by:

$$\begin{aligned} R' &= \{(a_1, a_2; c; r) : u \in_R \mathbb{Z}_n^*; a_1 \leftarrow g_1^u; a_2 \leftarrow g_2^u; r \leftarrow_n u + cx\}, \\ S' &= \{(a_1, a_2; c; r) : r \in_R \mathbb{Z}_n^*; a_1 \leftarrow g_1^r h_1^{-c}; a_2 \leftarrow g_2^r h_2^{-c}\}. \end{aligned}$$

c) *Determine both* $\Delta(R; R')$ *and* $\Delta(S; S')$.

d) *Show that* $\Delta(R'; S') \leq 2/n$ *using triangle inequalities for* Δ.

2. Let $\langle g \rangle$ be a cyclic group of order n.

Show that each of the following computational problems is random self-reducible.

a) *Given* g^x, g^y, g^z, *compute* $g^{xy^2z^4}$, *where* $x, y, z \in \mathbb{Z}_n^*$.

b) *Given* g^x, g^y, g^z, *compute* $g^{x+y^2+z^4}$, *where* $x, y \in \mathbb{Z}_n$ *and* $z \in \mathbb{Z}_n^*$.

3. Let $\langle g \rangle$ be a cyclic group of large prime order n. Let $h \in \langle g \rangle$ denote a random group element such that $\log_g h$ is unknown to anyone.
Consider relation R:

$$R = \{(A, B, C; x, y, z) : A = g^x \ \wedge \ B = h^y \wedge \ C = (gh)^{xyz} \wedge \ z \in \{1, -1\}\}.$$

a) *Give a* Σ*-protocol for relation* R *and prove that it is complete, special sound, and special honest-verifier zero-knowledge.*

b) *Let* H *be a cryptographic hash function. Turn your* Σ*-protocol into a noninteractive* Σ*-proof (using the Fiat-Shamir heuristic) and show how the* Σ*-proof is verified.*

4) Let $V = \{1, ..., n\}$ with $n \geq 1$.

Let S_n denote the set of permutations on V. Recall that for permutations $\pi, \pi' \in S_n$, their composition $\pi'' = \pi' \circ \pi$ satisfies $\pi''(x) = \pi'(\pi(x))$ for all $x \in V$. Also, for $\pi \in S_n$, its inverse π^{-1} satisfies $\pi^{-1}(\pi(x)) = \pi(\pi^{-1}(x)) = x$ for all $x \in V$.

Consider directed graphs $G = (V, E)$ all with the same vertex set $V = \{1, \ldots, n\}$ but arbitrary edge sets $E \subseteq V \times V$.

Two graphs $G_0 = (V, E_0)$ and $G_1 = (V, E_1)$ are **isomorphic** if there exists a permutation $\pi : V \to V$ such that $(x, y) \in E_0 \Leftrightarrow (\pi(x), \pi(y)) \in E_1$ holds for all $x, y \in V$. We write $G_1 = \pi(G_0)$ and also $G_0 = \pi^{-1}(G_1)$.

Computing such a permutation π given G_0 and G_1 is conjectured to be a hard problem (not in **BPP**).

Consider the following protocol for relation $\{(G_0, G_1; \pi) : G_1 = \pi(G_0)\}$, which proves that G_0 and G_1 are isomorphic and that the prover knows a permutation $\pi \in S_n$ mapping G_0 to G_1:

Prover		Verifier
$\upsilon \in_R S_n$ $H \leftarrow \upsilon(G_0)$		
	$\xrightarrow{H}$	
		$c \in_R \{0, 1\}$
	$\xleftarrow{c}$	
$\rho \leftarrow \begin{cases} \upsilon^{-1}, & \text{if } c = 0 \\ \pi \circ \upsilon^{-1}, & \text{if } c = 1 \end{cases}$		
	$\xrightarrow{\rho}$	
		$G_c \stackrel{?}{=} \rho(H)$

Show that the protocol is a Σ-protocol:

a) *Show that the protocol is complete.*

b) *Show that the protocol is special sound.*

c) *Show that the protocol is special honest-verifier zero-knowledge.*

1a: 3	1c: 3	2a: 6	3a: 11	4a: 3	4c: 4
1b: 3	1d: 3	2b: 6	3b: 3	4b: 5	

The final mark is the total number of points divided by 5, rounded to one decimal place.

Cryptographic Protocols (2DMI00)
Exam, June 23, 2021, 18:00–21:00h

Solve the following four problems, providing full motivation for the correctness of your solutions.

No calculators or any other electronic devices are allowed, nor any notes or books.

Please, hand in your answer pages, not your scratch paper.

1. Let $\langle g \rangle$ be a cyclic group of order n.

Let distributions X, Y, Z be given by:

$$\begin{aligned} X &= \{(g^x, g^{1/x}) : x \in_R \mathbb{Z}_n^*\}, \\ Y &= \{(g^x, g^y) : x \in_R \mathbb{Z}_n^*, y \in_R \mathbb{Z}_n\}, \\ Z &= \{(g^x, g^y) : x \in_R \mathbb{Z}_n^*, y \in_R \mathbb{Z}_n, y - 1/x \in \mathbb{Z}_n^*\}. \end{aligned}$$

Let Δ denote statistical distance.

a) *Assume n is prime. Determine $\Delta(X;Y)$, $\Delta(X;Z)$, and $\Delta(Y;Z)$.*

b) *Determine $\Delta(X;Y)$, $\Delta(X;Z)$, and $\Delta(Y;Z)$ for any n, $n \geq 2$.*

2. Let $\langle g \rangle$ be a cyclic group of order n.

Show that each of the following computational problems is random self-reducible.

a) *Given $g^x, g^y, g^{x^2/y}$, compute g^{x^3/y^2}, where $x, y \in \mathbb{Z}_n^*$.*

b) *Given $g^x, g^y, g^{x^2/y}$, compute g^{x^3/y^2}, where $x \in \mathbb{Z}_n$ and $y \in \mathbb{Z}_n^*$.*

3. Let $\langle g \rangle$ be a cyclic group of large prime order n.

Consider relation R:

$$R = \{(A, B, C; x, y) : A = g^x \ \wedge \ B = g^y \wedge \ y \neq 0 \ \wedge (C = g^{x/y} \vee C = g^{-x/y})\}.$$

a) *Give a Σ-protocol for relation R and prove that it is complete, special sound, and special honest-verifier zero-knowledge.*

b) *Let H be a cryptographic hash function. Turn your Σ-protocol into a noninteractive Σ-proof (using the Fiat-Shamir heuristic) and show how the Σ-proof is verified.*

4) Let $\langle g \rangle$ be a cyclic group of large prime order n. Let $h \in \langle g \rangle$ denote a random group element such that $\log_g h$ is unknown to anyone.

Recall Fermat's little theorem, which states that $x^n = x$ holds for all $x \in \mathbb{Z}_n$.

Consider the following protocol for relation $\{(A, B; x, y, z) : A = g^x h^y, B = g^{x^{n-1}} h^z\}$, which proves that B is a Pedersen commitment to a bit $x^{n-1} \in \{0, 1\}$ indicating whether the value x in the Pedersen commitment A is nonzero (or not):

Prover		Verifier
$t, u, v_1, v_2, w \in_R \mathbb{Z}_n$		
$C \leftarrow g^{x^{n-2}} h^t$		
$a_1 \leftarrow g^u h^{v_1}$		
$a_2 \leftarrow B^u h^{v_2}$		
$b \leftarrow C^u h^w$	$\xrightarrow{C, a_1, a_2, b}$	
$r \leftarrow_n u + cx$	$\xleftarrow{c}$	$c \in_R \mathbb{Z}_n$
$r_1 \leftarrow_n v_1 + cy$		
$r_2 \leftarrow_n v_2 + c(y - zx)$		
$s \leftarrow_n w + c(z - tx)$	$\xrightarrow{r, r_1, r_2, s}$	$g^r h^{r_1} \stackrel{?}{=} a_1 A^c$
		$B^r h^{r_2} \stackrel{?}{=} a_2 A^c$
		$C^r h^s \stackrel{?}{=} b B^c$

Show that the protocol is a Σ-protocol:

a) *Show that the protocol is complete.*

b) *Show that the protocol is special sound.*

c) *Show that the protocol is special honest-verifier zero-knowledge.*

1a: 6	2a: 6	3a: 11	4a: 3	4c: 3
1b: 6	2b: 6	3b: 3	4b: 6	

The final mark is the total number of points divided by 5, rounded to one decimal place.

Cryptographic Protocols (2DMI00)
Exam, April 16, 2021, 13:30–16:30h

Solve the following four problems, providing full motivation for the correctness of your solutions.

No calculators or any other electronic devices are allowed, nor any notes or books.

Please, hand in your answer pages, not your scratch paper.

1. Let $\langle g \rangle$ be a cyclic group of order n.

Let distributions X, Y, Z be given by:

$$\begin{aligned} X &= \{(g^x, g^y) : x \in_R \mathbb{Z}_n^*, y \in_R \mathbb{Z}_n\}, \\ Y &= \{(g^x, g^{1/x}) : x \in_R \mathbb{Z}_n^*\}, \\ Z &= \{(g^x, g^y) : x \in_R \mathbb{Z}_n^*, y \in_R \mathbb{Z}_n, y - 1/x \notin \mathbb{Z}_n^*\}. \end{aligned}$$

Let Δ denote statistical distance.

a) *Assume n is prime. Determine $\Delta(X;Y)$, $\Delta(X;Z)$, and $\Delta(Y;Z)$.*

b) *Determine $\Delta(X;Y)$, $\Delta(X;Z)$, and $\Delta(Y;Z)$ for any n, $n \geq 2$.*

2. Let $\langle g \rangle$ be a cyclic group of order n.

Show that each of the following computational problems is random self-reducible.

a) *Given $g^x, g^y, g^{x/y}$, compute $g^{x^2/y}$, where $x, y \in \mathbb{Z}_n^*$.*

b) *Given $g^x, g^y, g^{x/y}$, compute $g^{x^2/y}$, where $x \in \mathbb{Z}_n$ and $y \in \mathbb{Z}_n^*$.*

3. Let $\langle g \rangle$ be a cyclic group of large prime order n.

Consider relation R:

$$R = \{(A, B, C; x) : A = g^x \ \wedge \ (B = g^{-1/x} \ \vee \ C = g^{1/x}) \ \wedge \ x \neq 0\}.$$

a) *Give a Σ-protocol for relation R and prove that it is complete, special sound, and special honest-verifier zero-knowledge.*

b) *Let H be a cryptographic hash function. Turn your Σ-protocol into a non-interactive Σ-proof (using the Fiat-Shamir heuristic) and show how the Σ-proof is verified.*

4. Let $\langle g \rangle$ be a cyclic group of order n, where n is a large prime.

Let S be a nonempty subset of $\mathbb{Z}_n$.

Consider the following protocol for relation $\{(h; x) : h = g^x\}$:

Prover		Verifier
$u \in_R \mathbb{Z}_n^*$		
$a \leftarrow g^u$		
$b \in_R S$	$\xrightarrow{a,\, b}$	
	$\xleftarrow{c}$	$c \in_R \mathbb{Z}_n$
$r \leftarrow_n (b+c)u + x$	$\xrightarrow{r}$	
		$g^r \stackrel{?}{=} a^{b+c}h$

a) *Show that the protocol is complete.*

b) *Show that the protocol is special sound.*

Next, consider the case that $S = \{0\}$, hence $b = 0$ always holds in the protocol.

c) *Show that the protocol with $S = \{0\}$ cannot be special honest-verifier zero-knowledge under the DL assumption.*

However, the following simulation shows that the protocol with $S = \{0\}$ is actually (plain) honest-verifier zero-knowledge:

$$\left\{ (a, 0; c; r) : r \in_R \mathbb{Z}_n; \left\{ \begin{array}{ll} c \leftarrow 0; u \in_R \mathbb{Z}_n^*; a \leftarrow g^u, & \text{if } g^r = h \\ c \in_R \mathbb{Z}_n^*; a \leftarrow (g^r/h)^{1/c}, & \text{if } g^r \neq h \end{array} \right. \right\}.$$

Finally, consider the case that $S = \mathbb{Z}_n$.

d) *Show that the protocol with $S = \mathbb{Z}_n$ is special honest-verifier zero-knowledge by adapting the above simulation.*

1a: 6	2a: 6	3a: 11	4a: 1	4c: 4
1b: 6	2b: 6	3b: 3	4b: 3	4d: 4

The final mark is the total number of points divided by 5, rounded to one decimal place.

Cryptographic Protocols (2DMI00)
Exam, June 26, 2020, 18:00–21:00h

Solve the following four problems, providing full motivation for the correctness of your solutions.

No calculators or any other electronic devices are allowed, nor any notes or books.

Please, hand in your answer pages, not your scratch paper.

1) Let $\langle g \rangle$ be a cyclic group of order n.

Let distributions X, Y, Z be given by:

$$\begin{aligned} X &= \{(g^u, g^{uv}) : u \in_R \mathbb{Z}_n^*, v \in_R \mathbb{Z}_n\}, \\ Y &= \{(g^u, g^{uv}) : u, v \in_R \mathbb{Z}_n^*\}, \\ Z &= \{(g^u, g^{u/v}) : u, v \in_R \mathbb{Z}_n^*\}. \end{aligned}$$

Let Δ denote statistical distance.

a) *Assume n is prime. Determine $\Delta(X;Y)$, $\Delta(X;Z)$, and $\Delta(Y;Z)$.*

b) *Determine $\Delta(X;Y)$, $\Delta(X;Z)$, and $\Delta(Y;Z)$ for any n, $n \geq 2$.*

2) Let $\langle g \rangle$ be a cyclic group of order n.

Show that each of the following computational problems is random self-reducible.

a) *Given g^x, g^y, g^z, compute $g^{xy/z}$, where $x, y, z \in \mathbb{Z}_n^*$.*

b) *Given g^x, g^y, g^z, compute $g^{xy/z}$, where $x \in \mathbb{Z}_n$ and $y, z \in \mathbb{Z}_n^*$.*

3) Let $\langle g \rangle$ be a cyclic group of large prime order n. Let $h \in \langle g \rangle$ denote a random group element such that $\log_g h$ is unknown to anyone. Consider relation R:

$$R = \{(A, B, C; x, y) : A = g^x \ \wedge \ (B = g^{x^2} \ \vee \ B = g^{xy}) \ \wedge \ C = g^{-x} h^y\}.$$

a) *Give a Σ-protocol for relation R and prove that it is complete, special sound, and special honest-verifier zero-knowledge.*

b) *Let H be a cryptographic hash function. Turn your Σ-protocol into a non-interactive Σ-proof (using the Fiat-Shamir heuristic) and show how the Σ-proof is verified.*

4) Let $\langle g \rangle$ be a cyclic group of large prime order n. Let $h \in \langle g \rangle$ denote a random group element such that $\log_g h$ is unknown to anyone.

Recall Fermat's little theorem, which states that $x^n = x$ holds for all $x \in \mathbb{Z}_n$.

Consider the following protocol for relation $\{(A, B; x, y, z) : A = g^x h^y, B = g^{x^{n-1}} h^z\}$, which proves that B is a Pedersen commitment to a bit $x^{n-1} \in \{0, 1\}$ indicating whether the value x in the Pedersen commitment A is nonzero (or not):

Prover			Verifier
(case $x = 0$)	(case $x \neq 0$)		
$c_1, r_1, s_1, t_1, v_0, w_0 \in_R \mathbb{Z}_n$	$c_0, s_0, t_0, u_1, v_1, w_1 \in_R \mathbb{Z}_n$		
$a_0 \leftarrow h^{v_0}$	$a_0 \leftarrow h^{s_0} A^{-c_0}$		
$b_0 \leftarrow h^{w_0}$	$b_0 \leftarrow h^{t_0} B^{-c_0}$		
$a_1 \leftarrow A^{r_1} h^{s_1} g^{-c_1}$	$a_1 \leftarrow A^{u_1} h^{v_1}$		
$b_1 \leftarrow h^{t_1} (B/g)^{-c_1}$	$b_1 \leftarrow h^{w_1}$		
		$\xrightarrow{a_0, a_1, b_0, b_1}$	
			$c \in_R \mathbb{Z}_n$
		$\xleftarrow{c}$	
$c_0 \leftarrow_n c - c_1$	$c_1 \leftarrow_n c - c_0$		
	$r_1 \leftarrow_n u_1 + c_1/x$		
$s_0 \leftarrow_n v_0 + c_0 y$	$s_1 \leftarrow_n v_1 - c_1 y/x$		
$t_0 \leftarrow_n w_0 + c_0 z$	$t_1 \leftarrow_n w_1 + c_1 z$		
		$\xrightarrow{c_0, c_1, r_1, s_0, s_1, t_0, t_1}$	
			$c_0 + c_1 \stackrel{?}{=}_n c$
			$h^{s_0} \stackrel{?}{=} a_0 A^{c_0}$
			$h^{t_0} \stackrel{?}{=} b_0 B^{c_0}$
			$A^{r_1} h^{s_1} \stackrel{?}{=} a_1 g^{c_1}$
			$h^{t_1} \stackrel{?}{=} b_1 (B/g)^{c_1}$

Show that the protocol is a Σ-protocol:

a) *Show that the protocol is complete.*

b) *Show that the protocol is special sound.*

c) *Show that the protocol is special honest-verifier zero-knowledge.*

1a: 6	2a: 6	3a: 11	4a: 4	4c: 2
1b: 6	2b: 6	3b: 3	4b: 6	

The final mark is the total number of points divided by 5, rounded to one decimal place.

Cryptographic Protocols (2DMI00)
Exam, April 18, 2020, 13:30–16:30h

Solve the following four problems, providing full motivation for the correctness of your solutions.

No calculators or any other electronic devices are allowed, nor any notes or books.

Please, hand in your answer pages, not your scratch paper.

1) Let $\langle g \rangle$ be a cyclic group of order n.

Let distributions X, Y, Z be given by:

$$\begin{aligned} X &= \{(g^u, g^v) : u, v \in_R \mathbb{Z}_n\}, \\ Y &= \{(g^u, g^{uv}) : u \in_R \mathbb{Z}_n^*, v \in_R \mathbb{Z}_n\}, \\ Z &= \{(g^u, g^{uv}) : u, v \in_R \mathbb{Z}_n^*\}. \end{aligned}$$

Let Δ denote statistical distance.

a) *Assume n is prime. Determine $\Delta(X;Y)$, $\Delta(X;Z)$, and $\Delta(Y;Z)$.*

b) *Determine $\Delta(X;Y)$, $\Delta(X;Z)$, and $\Delta(Y;Z)$ for any n, $n \geq 1$.*

2) Let $\langle g \rangle$ be a cyclic group of order n.

Show that each of the following computational problems is random self-reducible.

a) *Given $g^x, g^{\frac{1}{x}}$, compute g^{x^2}, where $x \in \mathbb{Z}_n^*$.*

b) *Given $g^x, g^y, g^{\frac{1}{x+y}}$, compute $g^{\frac{x-y}{x+y}}$, where $x, y \in \mathbb{Z}_n$ and $x + y \in \mathbb{Z}_n^*$.*

3) Let $\langle g \rangle$ be a cyclic group of large prime order n. Let $h \in \langle g \rangle$ denote a random group element such that $\log_g h$ is unknown to anyone. Consider relation R:

$$R = \{(A, B, C; x, y) : A = g^x \ \wedge \ (B = g^{-x^2} \ \vee \ B = g^{x^2}) \ \wedge \ C = g^{x^3} h^y\}.$$

a) *Give a Σ-protocol for relation R and prove that it is complete, special sound, and special honest-verifier zero-knowledge.*

b) *Let H be a cryptographic hash function. Turn your Σ-protocol into a non-interactive Σ-proof (using the Fiat-Shamir heuristic) and show how the Σ-proof is verified.*

4) Let $\langle g \rangle$ be a cyclic group of large prime order n. Let $h \in \langle g \rangle$ denote a random group element such that $\log_g h$ is unknown to anyone.

Recall Fermat's little theorem, which states that $x^n = x$ holds for all $x \in \mathbb{Z}_n$.

Consider the following protocol for relation $\{(A, B; x, y, z) : A = g^x h^y, B = g^{x^{n-1}} h^z\}$, which proves that B is a Pedersen commitment to a bit $x^{n-1} \in \{0, 1\}$ indicating whether the value x in the Pedersen commitment A is nonzero (or not):

Prover		Verifier
$t, u, v_1, v_2, w \in_R \mathbb{Z}_n$		
$C \leftarrow g^{x^{n-2}} h^t$		
$a_1 \leftarrow g^u h^{v_1}$		
$a_2 \leftarrow B^u h^{v_2}$		
$b \leftarrow C^u h^w$	$\xrightarrow{C, a_1, a_2, b}$	
$r \leftarrow_n u + cx$	$\xleftarrow{c}$	$c \in_R \mathbb{Z}_n$
$r_1 \leftarrow_n v_1 + cy$		
$r_2 \leftarrow_n v_2 + c(y - zx)$		
$s \leftarrow_n w + c(z - tx)$	$\xrightarrow{r, r_1, r_2, s}$	$g^r h^{r_1} \stackrel{?}{=} a_1 A^c$
		$B^r h^{r_2} \stackrel{?}{=} a_2 A^c$
		$C^r h^s \stackrel{?}{=} b B^c$

Show that the protocol is a Σ-protocol:

a) *Show that the protocol is complete.*

b) *Show that the protocol is special sound.*

c) *Show that the protocol is special honest-verifier zero-knowledge.*

1a: 6	2a: 6	3a: 11	4a: 3	4c: 3
1b: 6	2b: 6	3b: 3	4b: 6	

The final mark is the total number of points divided by 5, rounded to one decimal place.

Cryptographic Protocols (2DMI00)
Exam, June 28, 2019, 18:00–21:00h

Solve the following four problems, providing full motivation for the correctness of your solutions.

Use of a simple, non-programmable pocket calculator is allowed, but not necessary.
Any other electronic equipment is not allowed, nor any notes or books.

Please, hand in your answer pages, not your scratch paper.

1) Let $\langle g \rangle$ be a cyclic group of order n.

For $n \geq 2$, let distributions X, Y, Z be given by:

$$\begin{aligned} X &= \{(g^x, g^{x^2}) : x \in_R \mathbb{Z}_n\}, \\ Y &= \{(g^x, g^y) : x, y \in_R \mathbb{Z}_n, y - x^2 \in \mathbb{Z}_n^*\}, \\ Z &= \{(g^x, g^y) : x, y \in_R \mathbb{Z}_n\}. \end{aligned}$$

Let Δ denote statistical distance.

a) *Assume n is prime. Determine $\Delta(X;Y)$, $\Delta(X;Z)$, and $\Delta(Y;Z)$.*

b) *Determine $\Delta(X;Y)$, $\Delta(X;Z)$, and $\Delta(Y;Z)$ for any n, $n \geq 2$.*

2) Let $\langle g \rangle$ be a cyclic group of order n.

Show that each of the following computational problems is random self-reducible.

a) *Given g^x, g^y, g^z, compute g^{xy/z^3}, where $x, y, z \in \mathbb{Z}_n^*$.*

b) *Given g^x, g^y, g^z, compute g^{xy+z^3}, where $x, y \in \mathbb{Z}_n$ and $z \in \mathbb{Z}_n^*$.*

3) Let $\langle g \rangle$ be a cyclic group of large prime order n. Let $h \in \langle g \rangle$ denote a random group element such that $\log_g h$ is unknown to anyone. Consider relation R:

$$R = \{(A, B, C; x, y) : A = g^x \ \wedge \ B = h^y \ \wedge \ (C = (gh)^{xy} \ \vee \ C = (gh)^{x+y})\}.$$

a) *Give a Σ-protocol for relation R and prove that it is complete, special sound, and special honest-verifier zero-knowledge.*

b) *Let H be a cryptographic hash function. Turn your Σ-protocol into a non-interactive Σ-proof (using the Fiat-Shamir heuristic) and show how the Σ-proof is verified.*

4) Let $\langle g \rangle$ be a cyclic group of large prime order n.

Consider the following protocol as a potential alternative to OR-composition of Schnorr's protocol. That is, the protocol is intended as a Σ-protocol for relation $\{(h_1, h_2; x_1, x_2) : h_1 = g^{x_1} \vee h_2 = g^{x_2}\}$.

Prover			Verifier
(using $x_1 = \log_g h_1$)	(using $x_2 = \log_g h_2$)		
$r_2, u_1 \in_R \mathbb{Z}_n$	$r_1, u_2 \in_R \mathbb{Z}_n$		
$a_1 \leftarrow g^{u_1}$	$a_1 \leftarrow g^{r_1}$		
$a_2 \leftarrow g^{r_2}$	$a_2 \leftarrow g^{u_2}$		
		$\xrightarrow{a_1, a_2}$	
			$c \in_R \mathbb{Z}_n$
		$\xleftarrow{c}$	
$r_1 \leftarrow_n u_1 + cx_1$	$r_2 \leftarrow_n u_2 + cx_2$		
		$\xrightarrow{r_1, r_2}$	
			$g^{r_1} \stackrel{?}{=} a_1 h_1^c \vee g^{r_2} \stackrel{?}{=} a_2 h_2^c$

a) *Show that the protocol is complete.*

b) *Determine if the protocol is special sound. If so, provide a proof; otherwise, show why not.*

c) *Determine if the protocol is special honest-verifier zero-knowledge. If so, provide a proof; otherwise, show why not.*

1a: 6	2a: 6	3a: 11	4a: 2	4c: 5
1b: 6	2b: 6	3b: 3	4b: 5	

The final mark is the total number of points divided by 5, rounded to one decimal place.

Cryptographic Protocols (2DMI00)
Exam, April 12, 2019, 13:30–16:30h

Solve the following four problems, providing full motivation for the correctness of your solutions.

Use of a simple, non-programmable pocket calculator is allowed, but not necessary.
Any other electronic equipment is not allowed, nor any notes or books.

Please, hand in your answer pages, not your scratch paper.

1) For $1 \leq d < n$, consider distributions X, Y, Z given by:

$$\begin{aligned} X &= \{u : u \in_R \{1, \ldots, dn\}\}, \\ Y &= \{un : u \in_R \{1, \ldots, d\}\}, \\ Z &= \{ud : u \in_R \{1, \ldots, n\}\}. \end{aligned}$$

Let Δ denote statistical distance.

a) *Determine* $\Delta(X; Y)$ *and* $\Delta(X; Z)$.

b) *Determine* $\Delta(Y; Z)$ *assuming that also* $\gcd(d, n) = 1$.

c) *Determine* $\Delta(Y; Z)$ *for arbitrary* d, n *with* $1 \leq d < n$.

2) Let $\langle g \rangle$ be a cyclic group of order n.

Show that each of the following computational problems is random self-reducible.

a) *Given* g^x, g^y, g^z, *compute* g^{x-yz}, *where* $x, y, z \in \mathbb{Z}_n$.

b) *Given* g^x, g^y, g^z, *compute* $g^{1/(x-yz)}$, *where* $x, y \in \mathbb{Z}_n$ *and* $z, x - yz \in \mathbb{Z}_n^*$.

3) Let $\langle g \rangle$ be a cyclic group of large prime order n. Let $h \in \langle g \rangle$ denote a random group element such that $\log_g h$ is unknown to anyone. Consider relation R:

$$R = \{(A, B; x, y) : A = g^x \ \wedge \ (B = g^{-2x} h^y \ \vee \ B = g^{x^2} h^y)\}.$$

a) *Give a* Σ*-protocol for relation* R *and prove that it is complete, special sound, and special honest-verifier zero-knowledge.*

b) *Let* H *be a cryptographic hash function. Turn your* Σ*-protocol into a non-interactive* Σ*-proof (using the Fiat-Shamir heuristic) and show how the* Σ*-proof is verified.*

4) Let $\langle g \rangle$ be a cyclic group of large prime order n.

Consider the following basic idea for constructing an (ℓ, ℓ)-threshold Schnorr signature scheme. Suppose parties $\mathcal{P}_i$ each hold a private key x_i and a public key $h_i = g^{x_i}$, for $1 \leq i \leq \ell$. Define $h = \prod_{i=1}^{\ell} h_i$ as the public key of parties $\mathcal{P}_1, \ldots, \mathcal{P}_\ell$ together.

For a given message M, the goal is to jointly generate a Schnorr signature (c, r) for public key h, where $c = H(g^r h^{-c}, M)$. Suppose party $\mathcal{C}$ acts as a "combiner," acting as the verifier in a run of the Schnorr protocol with each of the parties $\mathcal{P}_i$.

a) *Show how $\mathcal{C}$ can generate a Schnorr signature (c, r) on message M for public key h, by running the Schnorr protocol ℓ times in parallel, once with each party $\mathcal{P}_i$ for public key h_i. Argue why the scheme is secure.*
Hint: how should $\mathcal{C}$ choose the challenges c_i such that the conversations $(a_i; c_i; r_i)$ of the runs of the Schnorr protocol can be combined?

b) *Describe how your scheme can be extended to a (t, ℓ)-threshold Schnorr signature scheme, $1 \leq t \leq \ell$. You may assume that the parties have already run a distributed key generation protocol such that $\mathcal{P}_i$ holds a share x_i, where $x_i = a(i)$ for some polynomial $a(X) \in \mathbb{Z}_n[X]$ of degree less than t, and $x = a(0)$. As before, the public key of party $\mathcal{P}_i$ is $h_i = g^{x_i}$.*
Hint: how do you compute the public key $h = g^x$ from $h_1, \ldots, h_\ell$?

1a: 6	1c: 4	2a: 6	3a: 11	4a: 5
1b: 4		2b: 6	3b: 3	4b: 5

The final mark is the total number of points divided by 5, rounded to one decimal place.

Cryptographic Protocols (2DMI00)
Exam, July 3, 2018, 18:00–21:00h

Solve the following four problems, providing full motivation for the correctness of your solutions.

Use of a simple, non-programmable pocket calculator is allowed, but not necessary.
Any other electronic equipment is not allowed, nor any notes or books.

Please, hand in your answer pages, not your scratch paper.

1) Let $\langle g \rangle$ be a cyclic group of order n.

For $n \geq 2$, consider distributions X, Y^+, Y^-, Z^+, Z^- given by:

$$\begin{aligned}
X &= \{\ (g^u, g^v) : u, v \in_R \mathbb{Z}_n\ \}, \\
Y^+ &= \{\ (g^u, g^v) : u \in_R \mathbb{Z}_n;\ v \in_R \mathbb{Z}_n \setminus \{u\}\ \}, \\
Y^- &= \{\ (g^u, g^v) : u \in_R \mathbb{Z}_n;\ v \in_R \mathbb{Z}_n \setminus \{-u\}\ \}, \\
Z^+ &= \{\ (g^u, g^u) : u \in_R \mathbb{Z}_n\ \}, \\
Z^- &= \{\ (g^u, g^{-u}) : u \in_R \mathbb{Z}_n\ \}.
\end{aligned}$$

Let Δ denote statistical distance.

a) *Determine* $\Delta(X; Y^+)$, $\Delta(X; Z^+)$, $\Delta(Y^+; Z^+)$.

b) *Given your answers to part* **(a)**, *what are* $\Delta(X; Y^-)$, $\Delta(X; Z^-)$, $\Delta(Y^-; Z^-)$*?*

c) *Determine* $\Delta(Z^+; Z^-)$.

2) Let $\langle g \rangle$ be a cyclic group of order n.

Show that each of the following computational problems is random self-reducible.

a) *Given* g^x, g^y, *compute* $g^{(x+y)^2}$, *where* $x, y \in \mathbb{Z}_n$.

b) *Given* g^x, g^y, *compute* $g^{(x+y)^2}$, *where* $x, y \in \mathbb{Z}_n$ *and* $x + y \in \mathbb{Z}_n^*$.

3) Let $\langle g \rangle$ be a cyclic group of large prime order n. Consider relation R:

$$R = \{(A, B, C; x, y) : A = g^x \ \wedge\ B = g^y \ \wedge\ (C = g^{(x+y)^2} \ \vee\ C = g^{(x-y)^2})\}.$$

a) *Give a* Σ*-protocol for relation* R *and prove that it is complete, special sound, and special honest-verifier zero-knowledge.*

b) *Let* H *be a cryptographic hash function. Turn your* Σ*-protocol into a non-interactive* Σ*-proof (using the Fiat-Shamir heuristic) and show how the* Σ*-proof is verified.*

4) Let $\langle g \rangle$ be a cyclic group of large prime order n.

Consider the following protocols as potential alternatives to EQ-composition of Schnorr's protocol. That is, both protocols are intended as Σ-protocols for relation $R = \{(g_1, h_1, g_2, h_2; x) : h_1 = g_1^x, h_2 = g_2^x\}$.

Prover		Verifier
$(x = \log_{g_1} h_1,$ $x = \log_{g_2} h_2)$		
$u \in_R \mathbb{Z}_n$		
$a_1 \leftarrow g_1^u$		
$a_2 \leftarrow g_2^u$		
	$\xrightarrow{a_1, a_2}$	
		$c \in_R \mathbb{Z}_n$
	$\xleftarrow{c}$	
$r_1 \leftarrow_n u + cx$		
$r_2 \leftarrow_n u + cx$	$\xrightarrow{r_1, r_2}$	
		$g_1^{r_1} \stackrel{?}{=} a_1 h_1^c$
		$g_2^{r_2} \stackrel{?}{=} a_2 h_2^c$

Prover		Verifier
$(x = \log_{g_1} h_1,$ $x = \log_{g_2} h_2)$		
$r_1, r_2 \in_R \mathbb{Z}_n$		
	$\xrightarrow{r_1, r_2}$	
		$c \in_R \mathbb{Z}_n$
	$\xleftarrow{c}$	
$a_1 \leftarrow g_1^{r_1 - cx}$		
$a_2 \leftarrow g_2^{r_2 - cx}$	$\xrightarrow{a_1, a_2}$	
		$g_1^{r_1} \stackrel{?}{=} a_1 h_1^c$
		$g_2^{r_2} \stackrel{?}{=} a_2 h_2^c$

Note that $R \subseteq V \times W$, where $V = \langle g \rangle^* \times \langle g \rangle \times \langle g \rangle^* \times \langle g \rangle$ and $W = \mathbb{Z}_n$. Hence, for $(g_1, h_1, g_2, h_2; x) \in R$, we have that both g_1 and g_2 are generators of $\langle g \rangle$, h_1 and h_2 are arbitrary elements of $\langle g \rangle$, and x is an element of $\mathbb{Z}_n$ such that $x = \log_{g_1} h_1 = \log_{g_2} h_2$.

a) *Show that both protocols are complete.*

b) *For each of the protocols determine if it is special sound. If so, provide a proof; otherwise, show why not.*

c) *For each of the protocols determine if it is special honest-verifier zero-knowledge. If so, provide a proof; otherwise, show why not.*

1a: 6	1c: 4	2a: 6	3a: 11	4a: 2	4c: 5	homework
1b: 2		2b: 6	3b: 3	4b: 5		min. 0, max. 5

The final mark is the total number of points divided by 5, rounded to a multiple of 0.5, not exceeding 10.

Cryptographic Protocols (2DMI00)
Exam, April 20, 2018, 13:30–16:30h

Solve the following four problems, providing full motivation for the correctness of your solutions.

Use of a simple, non-programmable pocket calculator is allowed, but not necessary.
Any other electronic equipment is not allowed, nor any notes or books.

Please, hand in your answer pages, not your scratch paper.

1) Let $\langle g \rangle$ be a cyclic group of order n.

For $n \geq 2$, let distributions X, Y, Z be given by:

$$\begin{aligned} X &= \{(g^x, g^y, g^{xy}) : x, y \in_R \mathbb{Z}_n\}, \\ Y &= \{(g^x, g^y, g^z) : x, y, z \in_R \mathbb{Z}_n, z - xy \notin \mathbb{Z}_n^*\}, \\ Z &= \{(g^x, g^y, g^z) : x, y, z \in_R \mathbb{Z}_n\}. \end{aligned}$$

Let Δ denote statistical distance.

a) *Assume n is prime. Determine $\Delta(X;Y)$, $\Delta(X;Z)$, and $\Delta(Y;Z)$.*

b) *Determine $\Delta(X;Y)$, $\Delta(X;Z)$, and $\Delta(Y;Z)$ for any n, $n \geq 2$.*

2) Let $\langle g \rangle$ be a cyclic group of order n.

Show that each of the following computational problems is random self-reducible.

a) *Given g^x, g^y, g^z, compute $g^{x/(yz)}$, where $x, y, z \in \mathbb{Z}_n^*$.*

b) *Given g^x, g^y, g^z, compute $g^{x/(y+z)}$, where $x \in \mathbb{Z}_n^*$, $y, z \in \mathbb{Z}_n$, and $y + z \in \mathbb{Z}_n^*$.*

3) Let $\langle g \rangle$ be a cyclic group of large prime order n. Let $h \in \langle g \rangle$ denote a random group element such that $\log_g h$ is unknown to anyone. Consider relation R:

$$R = \{(A, B, C; x, y, z) : A = g^x \ \wedge \ B = h^y \ \wedge \ (C = g^{xy} h^z \ \vee \ C = g^z h^{xy})\}.$$

a) *Give a Σ-protocol for relation R and prove that it is complete, special sound, and special honest-verifier zero-knowledge.*

b) *Let H be a cryptographic hash function. Turn your Σ-protocol into a non-interactive Σ-proof (using the Fiat-Shamir heuristic) and show how the Σ-proof is verified.*

4) Let $\langle g \rangle$ be a cyclic group of large prime order n.

Consider the following protocols as potential alternatives to AND-composition of Schnorr's protocol. That is, the protocol is intended as a Σ-protocol for relation $R = \{(h_1, h_2; x_1, x_2) : h_1 = g^{x_1}, h_2 = g^{x_2}\}$.

Prover		Verifier
$(x_1 = \log_g h_1,$ $x_2 = \log_g h_2)$		
$r_1, r_2 \in_R \mathbb{Z}_n$		
	$\xrightarrow{r_1, r_2}$	
		$c \in_R \mathbb{Z}_n$
	$\xleftarrow{c}$	
$a_1 \leftarrow g^{r_1 - cx_1}$		
$a_2 \leftarrow g^{r_2 - cx_2}$	$\xrightarrow{a_1, a_2}$	
		$g^{r_1} \stackrel{?}{=} a_1 h_1^c$
		$g^{r_2} \stackrel{?}{=} a_2 h_2^c$

Prover		Verifier
$(x_1 = \log_g h_1,$ $x_2 = \log_g h_2)$		
$u \in_R \mathbb{Z}_n$		
$a_1 \leftarrow g^u$		
$a_2 \leftarrow g^u$		
	$\xrightarrow{a_1, a_2}$	
		$c \in_R \mathbb{Z}_n$
	$\xleftarrow{c}$	
$r_1 \leftarrow_n u + cx_1$		
$r_2 \leftarrow_n u + cx_2$	$\xrightarrow{r_1, r_2}$	
		$g^{r_1} \stackrel{?}{=} a_1 h_1^c$
		$g^{r_2} \stackrel{?}{=} a_2 h_2^c$

a) *Show that both protocols are complete.*

b) *For each of the protocols determine if it is special sound. If so, provide a proof; otherwise, show why not.*

c) *For each of the protocols determine if it is special honest-verifier zero-knowledge. If so, provide a proof; otherwise, show why not.*

1a: 6	2a: 6	3a: 12	4a: 2	4c: 4	homework
1b: 6	2b: 6	3b: 3	4b: 5		min. 0, max. 5

The final mark is the total number of points divided by 5, rounded to a multiple of 0.5, not exceeding 10.

Cryptographic Protocols (2DMI00)
Exam, June 30, 2017, 18:00–21:00h

Solve the following four problems, providing full motivation for the correctness of your solutions.

Use of a simple, non-programmable pocket calculator is allowed, but not necessary.
Any other electronic equipment is not allowed, nor any notes or books.

Please, hand in your answer pages, not your scratch paper.

1) Let $\langle g \rangle$ be a cyclic group of order n.

Let $h \in \langle g \rangle^*$, hence h is a generator of $\langle g \rangle$ as well.

Distributions X_s, Y_s, where $s \in \{1, -1\}$, are defined by:

$$\begin{aligned} X_s &= \{g^u h^s : u \in_R \mathbb{Z}_n\}, \\ Y_s &= \{g^u h^s : u \in_R \mathbb{Z}_n^*\}. \end{aligned}$$

Let Δ denote statistical distance.

a) *Determine* $\Delta(X_1; X_{-1})$.

b) *Assume* $n = p$, *where* $p > 2$ *is prime. Determine* $\Delta(Y_1; Y_{-1})$.

c) *Assume* $n = 2p$, *where* $p > 2$ *is prime. Determine* $\Delta(Y_1; Y_{-1})$.

2) Let $\langle g \rangle$ be a cyclic group of order n.

Show that each of the following computational problems is random self-reducible.

a) *Given* g^x, g^y, *compute* $g^{y^3/x}$, *where* $x, y \in \mathbb{Z}_n^*$.

b) *Given* g^x, g^y, *compute* $g^{1/(x-y)^2}$, *where* $x, y \in \mathbb{Z}_n$, $x - y \in \mathbb{Z}_n^*$.

3) Let $\langle g \rangle$ be a cyclic group of large prime order n. Consider relation R:

$$R = \{(A, B, C; x) : A = g^{x^2} \ \wedge \ ((B = g^x \wedge \ C = g^{x^3}) \ \vee \ (B = g^{x^3} \wedge C = g^x))\}.$$

a) *Give a* Σ*-protocol for relation* R *and prove that it is complete, special sound, and special honest-verifier zero-knowledge.*

b) *Let* H *be a cryptographic hash function. Turn your* Σ*-protocol into a non-interactive* Σ*-proof (using the Fiat-Shamir heuristic) and show how the* Σ*-proof is verified.*

4) Let $\langle g \rangle$ be a cyclic group of order n, where n is a large prime. Let $h \in \langle g \rangle$ denote a random group element such that $\log_g h$ is unknown to anyone.

Consider the following protocol for relation $\{(B; x, y) : B = g^x h^y \ \wedge \ x \in \{1, -1\}\}$:

Prover		Verifier
$u, v, w \in_R \mathbb{Z}_n$		
$a \leftarrow g^u h^v$		
$b \leftarrow B^u h^w$	$\xrightarrow{a, b}$	
		$c \in_R \mathbb{Z}_n$
	$\xleftarrow{c}$	
$r \leftarrow_n u + cx$		
$s \leftarrow_n v + cy$		
$t \leftarrow_n w - cxy$	$\xrightarrow{r, s, t}$	
		$g^r h^s \stackrel{?}{=} aB^c$
		$B^r h^t \stackrel{?}{=} bg^c$

Show that the protocol is a Σ-protocol:

a) *Show that the protocol is complete.*

b) *Show that the protocol is special sound.*

c) *Show that the protocol is special honest-verifier zero-knowledge.*

1a: 4	1c: 5	2a: 6	3a: 12	4a: 3	4c: 2	homework
1b: 4		2b: 6	3b: 3	4b: 5		min. 0, max. 5

The final mark is the total number of points divided by 5, rounded to a multiple of 0.5, not exceeding 10.

Cryptographic Protocols (2DMI00)
Exam, April 18, 2017, 9:00–12:00h

Solve the following four problems, providing full motivation for the correctness of your solutions.

Use of a simple, non-programmable pocket calculator is allowed, but not necessary.
Any other electronic equipment is not allowed, nor any notes or books.

Please, hand in your answer pages, not your scratch paper.

1) For $n \geq 1$, consider distributions X, Y, Z given by

$$\begin{aligned} X &= \{u : u \in_R \{0, \ldots, n-1\}\}, \\ Y &= \{3u : u \in_R \{0, \ldots, n-1\}\}, \\ Z &= \{3u+1 : u \in_R \{0, \ldots, n-1\}\}. \end{aligned}$$

Let Δ denote statistical distance.

a) *Determine* $\Delta(Y; Z)$.

b) *Determine* $\Delta(X; Y)$ *and* $\Delta(X; Z)$ *for* n *a multiple of* 3.

c) *Determine* $\Delta(X; Y)$ *for arbitrary* $n \geq 1$.

2) Let $\langle g \rangle$ be a cyclic group of order n.

Show that each of the following computational problems is random self-reducible.

a) *Given* g^x, g^y, *compute* g^{x+y}, *where* $x \in \mathbb{Z}_n$ *and* $y \in \mathbb{Z}_n^*$.

b) *Given* g^x, g^y, *compute* $g^{x^2+y^3}$, *where* $x \in \mathbb{Z}_n$ *and* $y \in \mathbb{Z}_n^*$.

3) Let $\langle g \rangle$ be a cyclic group of large prime order n. Let $h \in \langle g \rangle$ denote a random group element such that $\log_g h$ is unknown to anyone. Consider relation R:

$$R = \{(A, B, C; x, y) : A = g^x \ \wedge \ B = h^y \ \wedge \ (C = g^{x^2-y} \ \vee \ C = h^{xy})\}.$$

a) *Give a* Σ*-protocol for relation* R *and prove that it is complete, special sound, and special honest-verifier zero-knowledge.*

b) *Let* H *be a cryptographic hash function. Turn your* Σ*-protocol into a non-interactive* Σ*-proof (using the Fiat-Shamir heuristic) and show how the* Σ*-proof is verified.*

4) Let $\langle g \rangle$ be a cyclic group of order n, where n is a large prime. Let $h \in \langle g \rangle$ denote a random group element such that $\log_g h$ is unknown to anyone.

Consider the following protocol for relation $\{(B; x, y) : B = g^x h^y \ \wedge \ x \in \{0, 1\}\}$:

Prover		Verifier
$u, v, w \in_R \mathbb{Z}_n$		
$a \leftarrow g^u h^v$		
$b \leftarrow (B/g)^u h^w$	$\xrightarrow{a, b}$	
		$c \in_R \mathbb{Z}_n$
	$\xleftarrow{c}$	
$r \leftarrow_n u + cx$		
$s \leftarrow_n v + cy$		
$t \leftarrow_n w - cxy$	$\xrightarrow{r, s, t}$	
		$g^r h^s \stackrel{?}{=} aB^c$
		$(B/g)^r h^t \stackrel{?}{=} b$

Show that the protocol is a Σ-protocol:

a) *Show that the protocol is complete.*

b) *Show that the protocol is special sound.*

c) *Show that the protocol is special honest-verifier zero-knowledge.*

1a: 2	1c: 5	2a: 6	3a: 12	4a: 3	4c: 2	homework
1b: 6		2b: 6	3b: 3	4b: 5		min. 0, max. 5

The final mark is the total number of points divided by 5, rounded to a multiple of 0.5, not exceeding 10.

Cryptographic Protocols (2DMI00)
Exam, June 24, 2016, 18:00–21:00h

Solve the following four problems, providing full motivation for the correctness of your solutions.

Use of a simple, non-programmable pocket calculator is allowed, but not necessary.
Any other electronic equipment is not allowed, nor any notes or books.

Please, hand in your answer pages, not your scratch paper.

1) For $k, n \geq 1$ such that $n \leq 2^k$, consider distributions X and Y given by:

$$\begin{aligned} X &= \{u : u \in_R \mathbb{Z}_n\}, \\ Y &= \{u \bmod n : u \in_R \{0, \ldots, 2^k - 1\}\}. \end{aligned}$$

Let Δ denote statistical distance.

a) *Show that* $\Delta(X; Y) = 0$ *if* $n = 2^k$.

b) *Show that* $\Delta(X; Y) = \frac{(2^k \bmod n)(n-(2^k \bmod n))}{2^k n}$.

c) *Show that* $\Delta(X; Y) \leq n/2^k$.

Suppose k random bits $b_0 \in_R \{0, 1\}, \ldots, b_{k-1} \in_R \{0, 1\}$ are used to generate a random value modulo n by returning $z = (\sum_{i=0}^{k-1} b_i 2^i) \bmod n$ as output.

d) *Suggest a value for* k *as a function of* n *such that* z *is approximately uniformly distributed in* $\mathbb{Z}_n$.

2) Let $\langle g \rangle$ be a cyclic group of order n.

Show that each of the following computational problems is random self-reducible.

a) *Given* g^x, *compute* g^{1/x^3}, *where* $x \in \mathbb{Z}_n^*$.

b) *Given* g^x, g^{x^2}, *compute* g^{x^3}, *where* $x \in \mathbb{Z}_n$.

3) Let $\langle g \rangle$ be a cyclic group of large prime order n. Consider relation R:

$$R = \{(A, B, C; x) : A = g^x \ \wedge \ B = g^{x^2} \ \wedge \ (C = g^{x^3} \ \vee \ C = g^{-x^3})\}.$$

a) *Give a* Σ*-protocol for relation* R *and show that it is complete, special sound, and special honest-verifier zero-knowledge.*

b) *Let* H *be a cryptographic hash function. Turn your* Σ*-protocol into a non-interactive* Σ*-proof (using the Fiat-Shamir heuristic) and show how the* Σ*-proof is verified.*

4) Let $\langle g \rangle$ be a cyclic group of large prime order n.

Let $h \in \langle g \rangle$ denote a random group element such that $\log_g h$ is unknown to anyone.

Party $\mathcal{A}$ holds private input bits x_0, x_1 and party $\mathcal{B}$ holds a private input bit s.

Parties $\mathcal{A}$ and $\mathcal{B}$ run the following $\binom{2}{1}$-OT protocol such that party $\mathcal{B}$ obtains x_s as private output bit.

Party $\mathcal{A}$		Party $\mathcal{B}$
$(x_0, x_1 \in \{0,1\})$		$(s \in \{0,1\})$
		$u_{\mathcal{B}} \in_R \mathbb{Z}_n$
		$h_s \leftarrow g^{u_{\mathcal{B}}}$
		$h_{1-s} \leftarrow h/g^{u_{\mathcal{B}}}$
	$\xleftarrow{h_0, h_1}$	
$u_{\mathcal{A}} \in_R \mathbb{Z}_n$		
$(A, B_0, B_1) \leftarrow (g^{u_{\mathcal{A}}}, h_0^{u_{\mathcal{A}}} g^{x_0}, h_1^{u_{\mathcal{A}}} g^{x_1})$		
	$\xrightarrow{(A, B_0, B_1)}$	
		$x_s \leftarrow \log_g(B_s / A^{u_{\mathcal{B}}})$

First, assume that parties $\mathcal{A}$ and $\mathcal{B}$ are honest.

a) *Show that party $\mathcal{B}$ indeed obtains the intended value.*

b) *Argue why party $\mathcal{B}$ is not able to recover x_{1-s}—nor any other information than the value of x_s.*

Next, assume that party $\mathcal{B}$ is corrupt.

c) *Show how party $\mathcal{B}$ can break the protocol.*

d) *Assume that party $\mathcal{A}$ aborts the protocol if $h_0 h_1 = h$ does not hold. Show how party $\mathcal{B}$ can still break the protocol.*

1a: 2	1c: 3	2a: 6	3a: 11	4a: 2	4c: 3	homework
1b: 4	1d: 3	2b: 6	3b: 3	4b: 3	4d: 4	min. 0, max. 5

The final mark is the total number of points divided by 5, rounded to a multiple of 0.5, not exceeding 10.

Cryptographic Protocols (2DMI00)
Exam, April 8, 2016, 9:00–12:00h

Solve the following four problems, providing full motivation for the correctness of your solutions.

Use of a simple, non-programmable pocket calculator is allowed, but not necessary.
Any other electronic equipment is not allowed, nor any notes or books.

Please, hand in your answer pages, not your scratch paper.

1) Let $\langle g \rangle$ be a cyclic group of order n.

Let k denote the bit length of n, hence $2^{k-1} \leq n < 2^k$.

Distributions X and Y are defined by:

$$\begin{aligned} X &= \{g^x : x \in_R \mathbb{Z}_n\}, \\ Y &= \{g^x : x \in_R \{0, \ldots, 2^k - 1\}\}. \end{aligned}$$

Let Δ denote statistical distance.

a) *Show that* $\Delta(X;Y) = 0$ *if* $n = 2^{k-1}$.

b) *Show that* $\Delta(X;Y) = \frac{(2^k-n)(2n-2^k)}{2^k n}$.

Suppose k random bits $x_0 \in_R \{0,1\}, \ldots, x_{k-1} \in_R \{0,1\}$ are used to generate an element in $\langle g \rangle$ by returning $g^{\sum_{i=0}^{k-1} x_i 2^i}$ as output.

c) *Give an approximate analysis, in terms of* n *and* k*, to show when the statistical distance between the distribution of* $g^{\sum_{i=0}^{k-1} x_i 2^i}$ *and the uniform distribution on* $\langle g \rangle$ *is maximal.*

2) Let $\langle g \rangle$ be a cyclic group of order n.

Show that each of the following computational problems is random self-reducible.

a) *Given* g^x, g^y*, compute* $g^{(x-y)^2}$*, where* $x, y \in \mathbb{Z}_n$.

b) *Given* g^x, g^y*, compute* $g^{(x-y)^2}$*, where* $x, y \in \mathbb{Z}_n$ *and* $x - y \in \mathbb{Z}_n^*$.

3) Let $\langle g \rangle$ be a cyclic group of large prime order n. Consider relation R:

$$R = \{(A, B, C; x, y) : A = g^x \ \wedge \ B = g^y \ \wedge \ (C = g^{x^2-y^2} \ \vee \ C = g^{x^2+y^2})\}.$$

a) *Give a* Σ*-protocol for relation* R *and show that it is complete, special sound, and special honest-verifier zero-knowledge.*

b) *Let* H *be a cryptographic hash function. Turn your* Σ*-protocol into a non-interactive* Σ*-proof (using the Fiat-Shamir heuristic) and show how the* Σ*-proof is verified.*

4) Let $\langle g \rangle$ be a cyclic group of large prime order n.

Let h be a public key for a $(2,2)$-threshold homomorphic ElGamal cryptosystem used by two parties $\mathcal{A}$ and $\mathcal{B}$, which each hold one of the private shares of the corresponding private key.

Party $\mathcal{A}$ holds a private bit x and party $\mathcal{B}$ holds a private bit y.

Parties $\mathcal{A}$ and $\mathcal{B}$ run the following protocol (over a public channel) to securely multiply x and y.

Party $\mathcal{A}$		Party $\mathcal{B}$
$(x \in \{0,1\})$		$(y \in \{0,1\})$
$u \in_R \mathbb{Z}_n$ $A \leftarrow g^u$		
$B \leftarrow h^u g^x$	$\xrightarrow{(A,B)}$	$v \in_R \mathbb{Z}_n$ $C \leftarrow g^v A^y$
	$\xleftarrow{(C,D)}$	$D \leftarrow h^v B^y$
	$\xleftrightarrow{\text{jointly decrypt } (C,D)}$	
output xy		output xy

The output xy is public.

a) *Show that the protocol indeed outputs xy if $\mathcal{A}$ and $\mathcal{B}$ follow the protocol.*

b) *Show how party $\mathcal{A}$ can learn bit y by deviating from the protocol.*

c) *Show how an active adversary (not involving $\mathcal{A}$ or $\mathcal{B}$) can learn both bits x and y by attacking the protocol run between honest parties $\mathcal{A}$ and $\mathcal{B}$.*

1a: 3	1c: 3	2a: 6	3a: 11	4a: 3	4c: 5	homework
1b: 6		2b: 6	3b: 3	4b: 4		min. 0, max. 5

The final mark is the total number of points divided by 5, rounded to a multiple of 0.5, not exceeding 10.

Cryptography 2 (2XC13)/Cryptographic Protocols 1 (2WC17) Exam, Oct. 28, 2015, 1:30–4:30pm

Solve the following four problems, providing full motivation for the correctness of your solutions.

Use of a simple, non-programmable pocket calculator is allowed, but not necessary.
Any other electronic equipment is not allowed, nor any notes or books.

Please, hand in your answer pages, not your scratch paper.

1) For $n \geq 3$, consider distributions X_b, Y_b, for $b \in \{0,1\}$, given by:

$$\begin{aligned} X_b &= \{u + b : u \in_R \{1, \ldots, n\}\}, \\ Y_b &= \{u + (-1)^b : u \in_R \{1, \ldots, n\}\}. \end{aligned}$$

Let Δ denote statistical distance.

a) *Determine $\Delta(X_0; X_1)$ and $\Delta(Y_0; Y_1)$. Show that $\Delta(Y_0; Y_1) = 2\Delta(X_0; X_1)$.*

Now, consider the following symmetric cryptosystem. Given security parameter k, the key is generated as $K \in_R \{1, \ldots, 2^k\}$. For a plaintext $M \in \mathbb{Z}$, the ciphertext is computed as $C = M + K$. For a ciphertext $C \in \mathbb{Z}$, the plaintext is recovered as $M = C - K$.

Suppose the cryptosystem is used in either of these modes: mode (i) with plaintexts $M \in \{0,1\}$, or mode (ii) with plaintexts $M \in \{1,-1\}$.

b) *Assume an attacker knows which mode applies. Argue in terms of statistical distance, which mode is to be preferred.*

Consider the following protocol for sending a bit $b \in \{0,1\}$ from party $\mathcal{A}$ to party $\mathcal{B}$ over a public channel, where the security objective is to keep bit b hidden from any party other than $\mathcal{A}$ and $\mathcal{B}$.

Party $\mathcal{A}$		Party $\mathcal{B}$
$u_{\mathcal{A}} \in_R \{1, \ldots, 2^k\}$		
$c_{\mathcal{A}} \leftarrow b + u_{\mathcal{A}}$	$\xrightarrow{c_{\mathcal{A}}}$	$u_{\mathcal{B}} \in_R \{1, \ldots, 2^k\}$
	$\xleftarrow{c_{\mathcal{AB}}}$	$c_{\mathcal{AB}} \leftarrow c_{\mathcal{A}} + u_{\mathcal{B}}$
$c_{\mathcal{B}} \leftarrow c_{\mathcal{AB}} - u_{\mathcal{A}}$	$\xrightarrow{c_{\mathcal{B}}}$	$b' \leftarrow c_{\mathcal{B}} - u_{\mathcal{B}}$

c) *Verify that $b' = b$ if parties $\mathcal{A}$ and $\mathcal{B}$ follow the protocol.*

d) *Analyze whether the protocol is secure against passive attacks, and whether it is secure against active attacks.*

2) Let $\langle g \rangle$ be a cyclic group of order n.

Show that each of the following computational problems is random self-reducible.

a) *Given g^x, g^y, g^z, compute g^{x^2+yz}, where $x, y, z \in \mathbb{Z}_n$.*

b) *Given g^x, g^y, g^z, compute $g^{x^2+(y/z)^2}$, where $x \in \mathbb{Z}_n$ and $y, z \in \mathbb{Z}_n^*$.*

3) Let $\langle g \rangle$ be a cyclic group of large prime order n. Let $h \in \langle g \rangle$ denote a random group element such that $\log_g h$ is unknown to anyone. Consider relation R:

$$R = \{(A, B, C; x, y) : A = g^x \ \wedge \ B = h^y \ \wedge \ (C = g^{x^2} \ \vee \ C = h^{y^2})\}.$$

a) *Give a Σ-protocol for relation R and show that it is complete, special sound, and special honest-verifier zero-knowledge.*

b) *Let H be a cryptographic hash function. Turn your Σ-protocol into a non-interactive Σ-proof (using the Fiat-Shamir heuristic) and show how the Σ-proof is verified.*

4) Let $\langle g \rangle$ be a cyclic group of large prime order n.

Consider the following protocol as a potential alternative to EQ-composition of Schnorr's protocol. That is, the protocol is intended as a Σ-protocol for relation $R = \{(g_1, h_1, g_2, h_2; x) : h_1 = g_1^x, h_2 = g_2^x\}$.

Prover		Verifier
$(x = \log_{g_1} h_1 = \log_{g_2} h_2)$		
$u_1, u_2 \in_R \mathbb{Z}_n$		
$a_1 \leftarrow g_1^{u_1}$		
$a_2 \leftarrow g_2^{u_2}$		
	$\xrightarrow{a_1, a_2}$	
		$c \in_R \mathbb{Z}_n$
	$\xleftarrow{c}$	
$r_1 \leftarrow_n u_1 + cx$		
$r_2 \leftarrow_n u_2 + cx$		
	$\xrightarrow{r_1, r_2}$	
		$g_1^{r_1} \stackrel{?}{=} a_1 h_1^c$
		$g_2^{r_2} \stackrel{?}{=} a_2 h_2^c$

Note that $R \subseteq V \times W$, where $V = \langle g \rangle^* \times \langle g \rangle \times \langle g \rangle^* \times \langle g \rangle$ and $W = \mathbb{Z}_n$. Hence, for $(g_1, h_1, g_2, h_2; x) \in R$, we have that g_1 and g_2 are both generators of $\langle g \rangle$, h_1 and h_2 are arbitrary elements of $\langle g \rangle$, and x is an element of $\mathbb{Z}_n$ such that $x = \log_{g_1} h_1 = \log_{g_2} h_2$.

a) *Show that the protocol is complete.*

b) *Determine if the protocol is special sound. If so, provide a proof; otherwise, show why not.*

c) *Determine if the protocol is special honest-verifier zero-knowledge. If so, provide a proof; otherwise, show why not.*

1a: 4	1c: 1	2a: 6	3a: 11	4a: 2	4c: 5	homework
1b: 3	1d: 4	2b: 6	3b: 3	4b: 5		min. 0, max. 5

The final mark is the total number of points divided by 5, rounded to a multiple of 0.5 (for 2XC13) and rounded to an integer (for 2WC17), not exceeding 10.

Cryptography 2 (2XC13)/Cryptographic Protocols 1 (2WC17) Exam, June 25, 2015, 1:30–4:30pm

Solve the following four problems, providing full motivation for the correctness of your solutions.

Use of a simple, non-programmable pocket calculator is allowed, but not necessary.
Any other electronic equipment is not allowed, nor any notes or books.

Please, hand in your answer pages, not your scratch paper.

1) Let $\langle g \rangle$ be a cyclic group of order n.

Let $h \in \langle g \rangle^*$, hence h is a generator of $\langle g \rangle$ as well.

Distributions X_b, Y_b, where $b \in \{0, 1\}$, are defined by:

$$\begin{aligned} X_b &= \{g^u h^b : u \in_R \mathbb{Z}_n\}, \\ Y_b &= \{g^u h^b : u \in_R \mathbb{Z}_n^*\}. \end{aligned}$$

Let Δ denote statistical distance.

a) *Assume n is prime. Determine $\Delta(X_0; X_1)$ and $\Delta(Y_0; Y_1)$.*

b) *Assume $n = 2p$, where p is prime. Determine $\Delta(X_0; X_1)$ and $\Delta(Y_0; Y_1)$.*

c) *Does $\Delta(X_0; Y_0) = \Delta(X_1; Y_1)$ hold for arbitrary n? Explain your answer.*

2) Let $\langle g \rangle$ be a cyclic group of order n.

Show that each of the following computational problems is random self-reducible.

a) *Given g^x, g^y, g^z, compute g^{xy+z^2}, where $x, y, z \in \mathbb{Z}_n$.*

b) *Given g^x, g^y, g^z, compute $g^{xy+(1/z)^2}$, where $x, y \in \mathbb{Z}_n$ and $z \in \mathbb{Z}_n^*$.*

3) Let $\langle g \rangle$ be a cyclic group of large prime order n. Let $h \in \langle g \rangle$ denote a random group element such that $\log_g h$ is unknown to anyone. Consider relation R:

$$R = \{(A, B, C; x, y) : A = g^x \ \wedge \ B = h^y \ \wedge \ (C = g^{2x+y} \ \vee \ C = h^{2xy})\}.$$

a) *Give a Σ-protocol for relation R and show that it is complete, special sound, and special honest-verifier zero-knowledge.*

b) *Let H be a cryptographic hash function. Turn your Σ-protocol into a non-interactive Σ-proof (using the Fiat-Shamir heuristic) and show how the Σ-proof is verified.*

4) Let $\langle g \rangle$ be a cyclic group of large prime order n.

Consider the following protocol as a potential alternative to OR-composition of Schnorr's protocol. That is, the protocol is intended as a Σ-protocol for relation $\{(h_1, h_2; x_1, x_2) : h_1 = g^{x_1} \vee h_2 = g^{x_2}\}$.

Prover			Verifier
(using $x_1 = \log_g h_1$)	(using $x_2 = \log_g h_2$)		
$r_2, u_1 \in_R \mathbb{Z}_n$	$r_1, u_2 \in_R \mathbb{Z}_n$		
$a_1 \leftarrow g^{u_1}$	$a_1 \leftarrow g^{r_1}$		
$a_2 \leftarrow g^{r_2}$	$a_2 \leftarrow g^{u_2}$		
		$\xrightarrow{a_1, a_2}$	
			$c \in_R \mathbb{Z}_n$
		$\xleftarrow{c}$	
$r_1 \leftarrow_n u_1 + cx_1$	$r_2 \leftarrow_n u_2 + cx_2$		
		$\xrightarrow{r_1, r_2}$	
			$g^{r_1} \stackrel{?}{=} a_1 h_1^c \vee g^{r_2} \stackrel{?}{=} a_2 h_2^c$

a) *Show that the protocol is complete.*

b) *Determine if the protocol is special sound. If so, provide a proof; otherwise, show why not.*

c) *Determine if the protocol is special honest-verifier zero-knowledge. If so, provide a proof; otherwise, show why not.*

1a: 4	1c: 4	2a: 6	3a: 11	4a: 2	4c: 5	homework
1b: 4		2b: 6	3b: 3	4b: 5		min. 0, max. 5

The final mark is the total number of points divided by 5, rounded to a multiple of 0.5 (for 2XC13) and rounded to an integer (for 2WC17), not exceeding 10.

Cryptography 2 (2XC13)/Cryptographic Protocols 1 (2WC17) Exam, April 16, 2015, 1:30–4:30pm

Solve the following four problems, providing full motivation for the correctness of your solutions.

Use of a simple, non-programmable pocket calculator is allowed, but not necessary.
Any other electronic equipment is not allowed, nor any notes or books.

Please, hand in your answer pages, not your scratch paper.

1) Let $\langle g \rangle$ be a cyclic group of order n.

Let $x, y \in \mathbb{Z}_n^*$ be fixed.

Let distributions X, Y, Z be given by:

$$\begin{aligned} X &= \{(g^{xu}, g^{yu}) : u \in_R \mathbb{Z}_n^*\}, \\ Y &= \{(g^{xt}, g^{yu}) : t, u \in_R \mathbb{Z}_n^*\}, \\ Z &= \{(g^{t}, g^{u}) : t, u \in_R \mathbb{Z}_n^*\}. \end{aligned}$$

Let Δ denote statistical distance.

a) *Assume n is prime. Determine $\Delta(X;Y)$, $\Delta(X;Z)$, and $\Delta(Y;Z)$.*

b) *Determine $\Delta(X;Y)$, $\Delta(X;Z)$, and $\Delta(Y;Z)$ for arbitrary n.*

2) Let $\langle g \rangle$ be a cyclic group of order n.

Show that each of the following computational problems is random self-reducible.

a) *Given $g^x, g^y, g^{x/y}$, compute $g^{y/x}$, where $x, y \in \mathbb{Z}_n^*$.*

b) *Given g^x, g^y, compute $g^{1/(x+y)}$, where $x, y \in \mathbb{Z}_n$, $x + y \in \mathbb{Z}_n^*$.*

3) Let $\langle g \rangle$ be a cyclic group of large prime order n. Let $h \in \langle g \rangle$ denote a random group element such that $\log_g h$ is unknown to anyone. Consider relation R:

$$R = \{(A, B, C; x, y) : A = g^x \ \wedge \ B = h^y \ \wedge \ (C = g^{xy} \ \vee \ C = h^{x+y})\}.$$

a) *Give a Σ-protocol for relation R and show that it is complete, special sound, and special honest-verifier zero-knowledge.*

b) *Let H be a cryptographic hash function. Turn your Σ-protocol into a non-interactive Σ-proof (using the Fiat-Shamir heuristic) and show how the Σ-proof is verified.*

4) Let $\langle g \rangle$ be a cyclic group of large prime order n. Consider the following two protocols as variations of the Schnorr Σ-protocol for relation $\{(h; x) : h = g^x\}$:

Prover		Verifier
$(x = \log_g h)$		
$u \in_R \mathbb{Z}_n$		
$a \leftarrow g^u$		
	$\xrightarrow{a}$	
		$c \in_R \mathbb{Z}_n$
	$\xleftarrow{c}$	
$r \leftarrow_n 2u + cx$		
	$\xrightarrow{r}$	
		$g^r \stackrel{?}{=} a^2 h^c$

Prover		Verifier
$(x = \log_g h)$		
$u \in_R \mathbb{Z}_n$		
$a \leftarrow g^u$		
	$\xrightarrow{a}$	
		$c \in_R \mathbb{Z}_n$
	$\xleftarrow{c}$	
$r \leftarrow_n u + c^2 x$		
	$\xrightarrow{r}$	
		$g^r \stackrel{?}{=} a h^{c^2}$

a) *Show that both protocols are complete.*

b) *For each of the protocols determine if it is special sound. If so, provide a proof; otherwise, show why not.*

c) *For each of the protocols determine if it is special honest-verifier zero-knowledge. If so, provide a proof; otherwise, show why not.*

1a: 6	2a: 6	3a: 11	4a: 2	4c: 5	homework
1b: 6	2b: 6	3b: 3	4b: 5		min. 0, max. 5

The final mark is the total number of points divided by 5, rounded to a multiple of 0.5 (for 2XC13) and rounded to an integer (for 2WC17), not exceeding 10.

Cryptography 2 (2XC13)/Cryptographic Protocols 1 (2WC17) Exam, June 26, 2014, 2:00–5:00pm

Solve the following four problems, providing full motivation for the correctness of your solutions.

Use of a simple, non-programmable pocket calculator is allowed, but not necessary.
Any other electronic equipment is not allowed, nor any notes or books.

Please, hand in your answer pages, not your scratch paper.

1) Let $\langle g \rangle$ be a cyclic group of order n, $n \geq 2$.

Let distributions X, Y, Z be given by:

$$\begin{aligned} X &= \{(g^x, g^y, g^{xy}) : x, y \in_R \mathbb{Z}_n\}, \\ Y &= \{(g^x, g^y, g^z) : x, y, z \in_R \mathbb{Z}_n, z - xy \in \mathbb{Z}_n^*\}, \\ Z &= \{(g^x, g^y, g^z) : x, y, z \in_R \mathbb{Z}_n\}. \end{aligned}$$

Let Δ denote statistical distance.

a) *Assume n is prime. Determine $\Delta(X;Y)$, $\Delta(X;Z)$, and $\Delta(Y;Z)$.*

b) *Assume n is an arbitrary integer $n \geq 2$. Determine $\Delta(X;Y)$, $\Delta(X;Z)$, and $\Delta(Y;Z)$.*

2) Let $\langle g \rangle$ be a cyclic group of large prime order n.

Show that each of the following computational problems is random self-reducible.

a) *Given g^x, g^y, compute $g^{(x-1+y)^2}$, where $x, y \in \mathbb{Z}_n$.*

b) *Given g^x, g^y, compute $g^{(x-1)/y}$, where $x \in \mathbb{Z}_n \setminus \{1\}$ and $y \in \mathbb{Z}_n^*$.*

3) Let $\langle g \rangle$ be a cyclic group of large prime order n. Let $h \in \langle g \rangle$ denote a random group element such that $\log_g h$ is unknown to anyone. Consider relation R:

$$R = \{(A, B, C; x, y) : A = g^x \ \wedge \ B = g^y \ \wedge \ (C = h^{x+y} \ \vee \ C = h^{x-y})\}.$$

a) *Give a Σ-protocol for relation R and show that it is complete, special sound, and special honest-verifier zero-knowledge.*

b) *Let H be a cryptographic hash function. Turn your Σ-protocol into a non-interactive Σ-proof (using the Fiat-Shamir heuristic) and show how the Σ-proof is verified.*

4) Let $\langle g \rangle$ be a cyclic group of large prime order n. Consider the following two protocols as variations of the Schnorr Σ-protocol for relation $\{(h; x) : h = g^x\}$:

Prover		Verifier
$(x = \log_g h)$		
$u_1, u_2 \in_R \mathbb{Z}_n$		
$a_1 \leftarrow g^{u_1}$		
$a_2 \leftarrow g^{u_2}$		
	$\xrightarrow{a_1, a_2}$	
		$c_1, c_2 \in_R \mathbb{Z}_n$
	$\xleftarrow{c_1, c_2}$	
$r_1 \leftarrow_n u_1 + c_1 x$		
$r_2 \leftarrow_n u_2 + c_2 x$	$\xrightarrow{r_1, r_2}$	
		$g^{r_1} \stackrel{?}{=} a_1 h^{c_1}$
		$g^{r_2} \stackrel{?}{=} a_2 h^{c_2}$

Prover		Verifier
$(x = \log_g h)$		
$r_1, r_2 \in_R \mathbb{Z}_n$		
	$\xrightarrow{r_1, r_2}$	
		$c_1, c_2 \in_R \mathbb{Z}_n$
	$\xleftarrow{c_1, c_2}$	
$a_1 \leftarrow g^{r_1 - c_1 x}$		
$a_2 \leftarrow g^{r_2 - c_2 x}$	$\xrightarrow{a_1, a_2}$	
		$g^{r_1} \stackrel{?}{=} a_1 h^{c_1}$
		$g^{r_2} \stackrel{?}{=} a_2 h^{c_2}$

a) *Show that both protocols are complete.*

b) *For each of the protocols determine if it is special sound. If so, provide a proof; otherwise, show why not.*

c) *For each of the protocols determine if it is special honest-verifier zero-knowledge. If so, provide a proof; otherwise, show why not.*

1a: 6	2a: 6	3a: 11	4a: 2	4c: 5
1b: 6	2b: 6	3b: 3	4b: 5	

The final mark is the total number of points divided by 5, rounded to a multiple of 0.5 (for 2XC13) and rounded to an integer (for 2WC17).

Cryptography 2 (2XC13)/Cryptographic Protocols 1 (2WC17) Exam, April 17, 2014, 2:00–5:00pm

Solve the following four problems, providing full motivation for the correctness of your solutions.

Use of a simple, non-programmable pocket calculator is allowed, but not necessary.
Any other electronic equipment is not allowed, nor any notes or books.

Please, hand in your answer pages, not your scratch paper.

1) Let $\langle g \rangle$ be a cyclic group of large prime order n.
Consider the following parameterized Diffie-Hellman key exchange protocol:

Party $\mathcal{A}$		Party $\mathcal{B}$
$x_{\mathcal{A}} \in_R V_{\mathcal{A}}$		$x_{\mathcal{B}} \in_R V_{\mathcal{B}}$
$h_{\mathcal{A}} \leftarrow g^{x_{\mathcal{A}}}$		$h_{\mathcal{B}} \leftarrow g^{x_{\mathcal{B}}}$
	$\xrightarrow{h_{\mathcal{A}}}$	
	$\xleftarrow{h_{\mathcal{B}}}$	
$K \leftarrow h_{\mathcal{B}}^{x_{\mathcal{A}}}$		$K \leftarrow h_{\mathcal{A}}^{x_{\mathcal{B}}}$

Let distributions X and Y be given by:

$$\begin{aligned} X &= \{g^t : t \in_R \mathbb{Z}_n^*\}, \\ Y &= \{g^u : u \in_R \mathbb{Z}_n\}. \end{aligned}$$

Let Δ denote statistical distance.

a) *Determine* $\Delta(K; X)$ *if* $V_{\mathcal{A}} = \mathbb{Z}_n^*$ *and* $V_{\mathcal{B}} = \mathbb{Z}_n^*$.

b) *Determine* $\Delta(K; X)$ *and* $\Delta(K; Y)$ *if* $V_{\mathcal{A}} = \mathbb{Z}_n$ *and* $V_{\mathcal{B}} = \mathbb{Z}_n^*$.

c) *Determine* $\Delta(K; Y)$ *if* $V_{\mathcal{A}} = \mathbb{Z}_n$ *and* $V_{\mathcal{B}} = \mathbb{Z}_n$.

2) Let $\langle g \rangle$ be a cyclic group of large prime order n.

Show that each of the following computational problems is random self-reducible.

a) *Given* g^x, g^y, g^{xy}, *compute* $g^{\frac{1}{xy}}$, *where* $x, y \in \mathbb{Z}_n^*$.

b) *Given* g^x, g^y, *compute* $g^{(x-1)/y}$, *where* $x \in \mathbb{Z}_n$ *and* $y \in \mathbb{Z}_n^*$.

3) Let $\langle g \rangle$ be a cyclic group of large prime order n. Let $h \in \langle g \rangle$ denote a random group element such that $\log_g h$ is unknown to anyone. Consider relation R:

$$R = \{(A, B, C; x, y) : A = g^x \ \wedge \ B = g^y \ \wedge \ (C = h^x \ \vee \ C = h^y)\}.$$

a) *Give a Σ-protocol for relation R and show that it is complete, special sound, and special honest-verifier zero-knowledge.*

b) *Let H be a cryptographic hash function. Turn your Σ-protocol into a non-interactive Σ-proof (using the Fiat-Shamir heuristic) and show how the Σ-proof is verified.*

4) Let $\langle g \rangle$ be a cyclic group of large prime order n. Consider the following two protocols as variations of the Schnorr Σ-protocol for relation $\{(h; x) : h = g^x\}$:

Prover		Verifier
$(x = \log_g h)$		
$r \in_R \mathbb{Z}_n$		
	$\xrightarrow{\ r\ }$	
		$c_1, c_2 \in_R \mathbb{Z}_n$
	$\xleftarrow{\ c_1, c_2\ }$	
$a_1 \leftarrow g^{r - c_1 x}$		
$a_2 \leftarrow g^{r - c_2 x}$	$\xrightarrow{\ a_1, a_2\ }$	
		$g^r \stackrel{?}{=} a_1 h^{c_1}$
		$g^r \stackrel{?}{=} a_2 h^{c_2}$

Prover		Verifier
$(x = \log_g h)$		
$u \in_R \mathbb{Z}_n$		
$a \leftarrow g^u$		
	$\xrightarrow{\ a\ }$	
		$c_1, c_2 \in_R \mathbb{Z}_n$
	$\xleftarrow{\ c_1, c_2\ }$	
$r_1 \leftarrow_n u + c_1 x$		
$r_2 \leftarrow_n u + c_2 x$	$\xrightarrow{\ r_1, r_2\ }$	
		$g^{r_1} \stackrel{?}{=} a h^{c_1}$
		$g^{r_2} \stackrel{?}{=} a h^{c_2}$

a) *Show that both protocols are complete.*

b) *For each of the protocols determine if it is special sound. If so, provide a proof; otherwise, show why not.*

c) *For each of the protocols determine if it is special honest-verifier zero-knowledge. If so, provide a proof; otherwise, show why not.*

1a: 3	1c: 3	2a: 6	3a: 11	4a: 2	4c: 5
1b: 6		2b: 6	3b: 3	4b: 5	

The final mark is the total number of points divided by 5, rounded to a multiple of 0.5 (for 2XC13) and rounded to an integer (for 2WC17).

Cryptography 2 (2XC13)/Cryptographic Protocols 1 (2WC17) Exam, June 25, 2013, 2:00–5:00pm

Solve the following four problems, providing full motivation for the correctness of your solutions.

Use of a simple, non-programmable pocket calculator is allowed, but not necessary.
Any other electronic equipment is not allowed, nor any notes or books.

Please, hand in your answer pages, not your scratch paper.

1) For integer $n \geq 3$, consider distributions X_b, Y_b, $b \in \{0,1\}$, given by:

$$\begin{aligned} X_b &= \{u + b : u \in_R \{1, \ldots, n\}\}, \\ Y_b &= \{u + (-1)^b : u \in_R \{1, \ldots, n\}\}. \end{aligned}$$

Let Δ denote statistical distance.

a) *Determine $\Delta(X_0; X_1)$ and $\Delta(Y_0; Y_1)$. Show that $\Delta(Y_0; Y_1) = 2\Delta(X_0; X_1)$.*

Now, consider the following symmetric cryptosystem. Given security parameter k, the key is generated as $K \in_R \{1, \ldots, 2^k\}$. For a plaintext $M \in \mathbb{Z}$, the ciphertext is computed as $C = M + K$. For a ciphertext $C \in \mathbb{Z}$, the plaintext is recovered as $M = C - K$.

Suppose the cryptosystem is used in either of these modes: mode (i) with plaintexts $M \in \{0, 1\}$, or mode (ii) with plaintexts $M \in \{1, -1\}$.

b) *Assume an attacker knows which mode applies. Argue in terms of statistical distance, which mode is to be preferred.*

Consider the following protocol for sending a bit $b \in \{0, 1\}$ from party $\mathcal{A}$ to party $\mathcal{B}$ over a public channel, where the security objective is to keep bit b hidden from any party other than $\mathcal{A}$ and $\mathcal{B}$.

Party $\mathcal{A}$		Party $\mathcal{B}$
$u_{\mathcal{A}} \in_R \{1, \ldots, 2^k\}$		
$c_{\mathcal{A}} \leftarrow b + u_{\mathcal{A}}$	$\xrightarrow{c_{\mathcal{A}}}$	$u_{\mathcal{B}} \in_R \{1, \ldots, 2^k\}$
	$\xleftarrow{c_{\mathcal{AB}}}$	$c_{\mathcal{AB}} \leftarrow c_{\mathcal{A}} + u_{\mathcal{B}}$
$c_{\mathcal{B}} \leftarrow c_{\mathcal{AB}} - u_{\mathcal{A}}$	$\xrightarrow{c_{\mathcal{B}}}$	$b' \leftarrow c_{\mathcal{B}} - u_{\mathcal{B}}$

c) *Verify that $b' = b$ if parties $\mathcal{A}$ and $\mathcal{B}$ follow the protocol.*

d) *Analyze whether the protocol is secure against passive attacks, and whether it is secure against active attacks.*

2) Let $\langle g \rangle$ be a cyclic group of order n, where n is a large prime.

Show that each of the following computational problems is random self-reducible.

a) *Given $g^x, g^y, g^{\frac{1}{xy}}$, compute g^{xy}, where $x, y \in \mathbb{Z}_n^*$.*

b) *Given g^x, g^y, compute $g^{x^2+y^2}$, where $x \in \mathbb{Z}_n$ and $y \in \mathbb{Z}_n^*$.*

3) Let $\langle g \rangle$ be a cyclic group of order n, where n is a large prime. Let $h \in \langle g \rangle$ denote a random group element such that $\log_g h$ is unknown to anyone. Consider relation R:

$$R = \{(A, B, C; x, y) : A = g^x \ \wedge \ B = h^y \ \wedge \ (C = g^{xy} \ \vee \ C = h^{xy})\}.$$

a) *Give a Σ-protocol for relation R and show that it is complete, special sound, and special honest-verifier zero-knowledge.*

b) *Let H be a cryptographic hash function. Turn your Σ-protocol into a non-interactive Σ-proof (using the Fiat-Shamir heuristic) and show how the Σ-proof is verified.*

4) Let $\langle g \rangle$ be a cyclic group of prime order n. Consider the following two protocols as variations of the Schnorr Σ-protocol for relation $\{(h; x) : h = g^x\}$:

Prover		Verifier
$(x = \log_g h)$		
$u \in_R \mathbb{Z}_n$		
	$\xrightarrow{\quad u \quad}$	
		$c \in_R \mathbb{Z}_n$
	$\xleftarrow{\quad c \quad}$	
$r \leftarrow_n u + cx$		
	$\xrightarrow{\quad r \quad}$	
		$g^r \stackrel{?}{=} g^u h^c$

Prover		Verifier
$(x = \log_g h)$		
$r \in_R \mathbb{Z}_n$		
	$\xrightarrow{\quad r \quad}$	
		$c \in_R \mathbb{Z}_n$
	$\xleftarrow{\quad c \quad}$	
$a \leftarrow g^{r-cx}$		
	$\xrightarrow{\quad a \quad}$	
		$g^r \stackrel{?}{=} ah^c$

a) *Show that both protocols are complete.*

b) *For each of the protocols determine if it is special sound. If so, provide a proof; otherwise, show why not.*

c) *For each of the protocols determine if it is special honest-verifier zero-knowledge. If so, provide a proof; otherwise, show why not.*

1a: 4	1c: 1	2a: 6	3a: 11	4a: 2	4c: 5
1b: 3	1d: 4	2b: 6	3b: 3	4b: 5	

The final mark is the total number of points divided by 5, rounded to a multiple of 0.5 (for 2XC13) and rounded to an integer (for 2WC17).

Cryptography 2 (2XC13)/Cryptographic Protocols 1 (2WC17) Exam, April 11, 2013, 2:00–5:00pm

---

Solve the following four problems, providing full motivation for the correctness and completeness of your solutions.

Use of a simple, non-programmable pocket calculator is allowed, but not necessary. All other electronic equipment is not allowed, nor any notes or books.

Hand in your answer pages, not your scratch paper. GOOD LUCK!

---

1) Let $\langle g \rangle$ be a cyclic group of order n, where n is prime. Let $g_1, g_2, h_1, h_2 \in \langle g \rangle \setminus \{1\}$. For fixed $c \in \mathbb{Z}_n^*$, consider distributions R, S given by:

$$\begin{aligned} R &= \{(a_1, a_2; c; r) : u \in_R \mathbb{Z}_n; a_1 \leftarrow g_1^u; a_2 \leftarrow g_2^u; r \leftarrow_n u + cx\}, \\ S &= \{(a_1, a_2; c; r) : r \in_R \mathbb{Z}_n; a_1 \leftarrow g_1^r h_1^{-c}; a_2 \leftarrow g_2^r h_2^{-c}\}. \end{aligned}$$

Let Δ denote statistical distance.

a) *Determine* $\Delta(R; S)$ *if* $\log_{g_1} h_1 = \log_{g_2} h_2$.

b) *Determine* $\Delta(R; S)$ *if* $\log_{g_1} h_1 \neq \log_{g_2} h_2$.

Next, assume $\log_{g_1} h_1 = \log_{g_2} h_2$. For fixed $c \in \mathbb{Z}_n^*$, consider also distributions R', S' given by:

$$\begin{aligned} R' &= \{(a_1, a_2; c; r) : u \in_R \mathbb{Z}_n^*; a_1 \leftarrow g_1^u; a_2 \leftarrow g_2^u; r \leftarrow_n u + cx\}, \\ S' &= \{(a_1, a_2; c; r) : r \in_R \mathbb{Z}_n^*; a_1 \leftarrow g_1^r h_1^{-c}; a_2 \leftarrow g_2^r h_2^{-c}\}. \end{aligned}$$

c) *Determine both* $\Delta(R; R')$ *and* $\Delta(S; S')$.

d) *Show that* $\Delta(R'; S') \leq 2/n$ *using triangle inequalities for* Δ.

2) Let $\langle g \rangle$ be a cyclic group of order n, where n is a large prime.

Show that each of the following computational problems is random self-reducible.

a) *Given* g^x, g^y, *compute* $g^{x^2/y}$, *where* $x, y \in \mathbb{Z}_n^*$.

b) *Given* g^x, g^y, *compute* $g^{x/y}$, *where* $x \in \mathbb{Z}_n$ *and* $y \in \mathbb{Z}_n^*$.

3) Let $\langle g \rangle$ be a cyclic group of order n, where n is a large prime. Consider relation R:

$$R = \{(A, B, C; x, y) : (A = g^x \ \vee \ B = g^y) \ \wedge \ C = g^{xy}\}.$$

a) *Give a Σ-protocol for relation R and show that it is complete, special sound, and special honest-verifier zero-knowledge.*

b) *Let H be a cryptographic hash function. Turn your Σ-protocol into a non-interactive Σ-proof (using the Fiat-Shamir heuristic) and show how the proof is verified.*

4) Let $\langle g \rangle$ be a cyclic group of prime order n. Let $g_1, g_2, h_1, h_2 \in \langle g \rangle \setminus \{1\}$. Consider the following Σ-protocol for relation $\{(g_1, h_1, g_2, h_2; x_1, x_2) : h_1 = g_1^{x_1}, h_2 = g_2^{x_2}\}$.

Prover			Verifier
$((x_1, x_2) = (\log_g h_1, \log_g h_2))$			
(if $x_1 = x_2$)	(if $x_1 \neq x_2$)		
$u_1 \in_R \mathbb{Z}_n$	$c_1, r_1 \in_R \mathbb{Z}_n$		
$a_{11} \leftarrow g_1^{u_1}$	$a_{11} \leftarrow g_1^{r_1} h_1^{-c_1}$		
$a_{12} \leftarrow g_2^{u_1}$	$a_{12} \leftarrow g_2^{r_1} h_2^{-c_1}$		
$c_2, r_{21}, r_{22}, r_{23}, r_{24} \in_R \mathbb{Z}_n$	$u_{21}, u_{22}, u_{23}, u_{24} \in_R \mathbb{Z}_n$		
$a_{21} \leftarrow g_1^{r_{21}} h_1^{-c_2}$	$a_{21} \leftarrow g_1^{u_{21}}$		
$a_{22} \leftarrow g_2^{r_{22}} h_2^{-c_2}$	$a_{22} \leftarrow g_2^{u_{22}}$		
$a_{23} \leftarrow (g_1 g_2)^{r_{23}} (h_1 h_2)^{r_{24}} g_2^{-c_2}$	$a_{23} \leftarrow (g_1 g_2)^{u_{23}} (h_1 h_2)^{u_{24}}$	$\xrightarrow{a_{11}, a_{12}, a_{21}, a_{22}, a_{23}}$	
			$c \in_R \mathbb{Z}_n$
$c_1 \leftarrow_n c - c_2$	$c_2 \leftarrow_n c - c_1$	$\xleftarrow{c}$	
$r_1 \leftarrow_n u_1 + c_1 x_1$	$r_{21} \leftarrow_n u_{21} + c_2 x_1$		
	$r_{22} \leftarrow_n u_{22} + c_2 x_2$		
	$r_{23} \leftarrow_n u_{23} + c_2 x_1 / (x_1 - x_2)$		
	$r_{24} \leftarrow_n u_{24} + c_2 / (x_2 - x_1)$	$\xrightarrow{c_1, c_2, r_1, r_{21}, r_{22}, r_{23}, r_{24}}$	$c_1 + c_2 \stackrel{?}{=}_n c$
			$g_1^{r_1} \stackrel{?}{=} a_{11} h_1^{c_1}$
			$g_2^{r_1} \stackrel{?}{=} a_{12} h_2^{c_1}$
			$g_1^{r_{21}} \stackrel{?}{=} a_{21} h_1^{c_2}$
			$g_2^{r_{22}} \stackrel{?}{=} a_{22} h_2^{c_2}$
			$(g_1 g_2)^{r_{23}} (h_1 h_2)^{r_{24}} \stackrel{?}{=} a_{23} g_2^{c_2}$

a) *Show that the protocol is complete.*

b) *Show that the protocol is special sound.*

c) *Show that the protocol is special honest-verifier zero-knowledge.*

1a: 3	1c: 4	2a: 6	3a: 12	4a: 2	4c: 4
1b: 3	1d: 3	2b: 6	3b: 3	4b: 4	

The final mark is the total number of points divided by 5, rounded to a multiple of 0.5 (for 2XC13) and rounded to an integer (for 2WC17).

Cryptography 2 (2XC13) / Cryptographic Protocols (2XC10)
Exam, June 25, 2012, 2:00–5:00pm

Solve the following four problems, providing full motivation for the correctness and completeness of your solutions.

Use of a simple, non-programmable pocket calculator is allowed, but not necessary. All other electronic equipment is not allowed, nor any notes or books.

Hand in your answer pages, not your scratch paper. GOOD LUCK!

---

1) For integer $n \geq 1$, consider distributions U, U^+, U^- given by:

$$\begin{aligned} U &= \{\ u : u \in_R \{1, \ldots, n\}\ \}, \\ U^+ &= \{\ u + b : u \in_R \{1, \ldots, n\}, b \in_R \{0, 1\}\}, \\ U^- &= \{\ u - b : u \in_R \{1, \ldots, n\}, b \in_R \{0, 1\}\}. \end{aligned}$$

Let Δ denote statistical distance.

a) *Determine* $\Delta(U; U^+)$, $\Delta(U; U^-)$, *and* $\Delta(U^+; U^-)$.

Let X and Y be random variables taking on values in a finite set V.

b) *Show that* $|\Pr[X = v] - \Pr[Y = v]| \leq \Delta(X; Y)$ *for all* $v \in V$.

c) *Does* $\Delta(X; Y) = \max_{v \in V} |\Pr[X = v] - \Pr[Y = v]|$ *hold in general? Explain your answer.*

2) Let $\langle g \rangle$ be a cyclic group of order n, where n is a large prime.

Show that each of the following computational problems is random self-reducible.

a) *Given* g^x, g^y, *compute* $g^{(x-y)^2}$, *where* $x, y \in \mathbb{Z}_n$.

b) *Given* g^x, g^y, *compute* $g^{1/(x-y)}$, *where* $x, y \in \mathbb{Z}_n$ *and* $x \neq y$.

3) Let $\langle g \rangle$ be a cyclic group of order n, where n is a large prime.

Consider the relation R given by

$$R = \{(A, B, C; x, y) : A = g^x \ \wedge \ B = g^y \ \wedge \ (C = g^{x^2} \ \vee \ C = g^{y^2})\}.$$

a) *Give a Σ-protocol for relation R and show that it is complete, special sound, and special honest-verifier zero-knowledge.*

b) *Let H denote a cryptographic hash function. Turn the above Σ-protocol into a non-interactive Σ-proof (using the Fiat-Shamir heuristic) and show how the proof is verified.*

4) Let $\langle g \rangle$ be a cyclic group of order n, where n is a large prime. Let $h \in \langle g \rangle$ denote a random group element such that $\log_g h$ is unknown to anyone.

Consider the following protocol for relation $\{(B; x, y) : B = g^x h^y \ \wedge \ xy = 1\}$:

Prover		Verifier
$u, v, w \in_R \mathbb{Z}_n$		
$a \leftarrow g^u h^v$		
$b \leftarrow g^w B^u$	$\xrightarrow{a, b}$	
		$c \in_R \mathbb{Z}_n$
	$\xleftarrow{c}$	
$r \leftarrow_n u + cx$		
$s \leftarrow_n v + cy$		
$t \leftarrow_n w - cx^2$	$\xrightarrow{r, s, t}$	
		$g^r h^s \stackrel{?}{=} aB^c$
		$g^t B^r \stackrel{?}{=} bh^c$

a) *Show that the protocol is a Σ-protocol.*

b) *What happens if the challenge is generated as $c = H(a, b)$ (hence omitting B from the input to H) to obtain a non-interactive Σ-proof? Is it secure? Explain your answer.*

1a: 6	1c: 3	2a: 6	3a: 11	4a: 6
1b: 4		2b: 6	3b: 3	4b: 5

The final mark is the total number of points divided by 5, rounded to a multiple of 0.5, not exceeding 10.

Cryptography 2 (2XC13) / Cryptographic Protocols (2XC10)
Exam, April 16, 2012, 2:00–5:00pm

Solve the following four problems, providing full motivation for the correctness and completeness of your solution.

Use of a simple, non-programmable pocket calculator is allowed, but not necessary. All other electronic equipment is not allowed, nor any notes or books.

Hand in your answer pages, not your scratch paper. GOOD LUCK!

---

1) For integer $n \geq 2$, consider distributions X, Y^+, Z^+, Y^-, Z^- given by:

$$\begin{aligned}
X &= \{\ (u,v) : u, v \in_R \mathbb{Z}_n\ \}, \\
Y^+ &= \{\ (u,v) : u \in_R \mathbb{Z}_n;\ v \in_R \mathbb{Z}_n \setminus \{u\}\ \}, \\
Z^+ &= \{\ (u,u) : u \in_R \mathbb{Z}_n\ \}, \\
Y^- &= \{\ (u,v) : u \in_R \mathbb{Z}_n;\ v \in_R \mathbb{Z}_n \setminus \{-u\}\ \}, \\
Z^- &= \{\ (u,-u) : u \in_R \mathbb{Z}_n\ \}.
\end{aligned}$$

Let Δ denote statistical distance.

a) *Determine* $\Delta(X, Y^+)$, $\Delta(X, Z^+)$, $\Delta(Y^+, Z^+)$.

b) *Given the answer to part* **(a)**, *what are* $\Delta(X, Y^-)$, $\Delta(X, Z^-)$, $\Delta(Y^-, Z^-)$*?*

c) *Determine* $\Delta(Z^+, Z^-)$.

2) Let $\langle g \rangle$ be a cyclic group of order n, where n is a large prime.

Show that each of the following computational problems is random self-reducible.

a) *Given* g^x, g^y, *compute* $g^{x/y}$, *where* $x, y \in \mathbb{Z}_n^*$.

b) *Given* g^x, g^y, *compute* $g^{x+1/y}$, *where* $x \in \mathbb{Z}_n$ *and* $y \in \mathbb{Z}_n^*$.

3) Let $\langle g \rangle$ be a cyclic group of order n, where n is a large prime. Let $h \in \langle g \rangle$ denote a random group element such that $\log_g h$ is unknown to anyone.

Consider the relation R given by

$$R = \{(A, B, C; x, y) : A = g^x \ \wedge \ (B = g^x h^y \ \vee \ C = g^{x^2} h^y)\}.$$

a) *Give a Σ-protocol for relation R and show that it is complete, special sound, and special honest-verifier zero-knowledge.*

b) *Let H denote a cryptographic hash function. Turn the above Σ-protocol into a non-interactive Σ-proof (using the Fiat-Shamir heuristic) and show how the proof is verified.*

4) Let $\langle g \rangle$ be a cyclic group of order n, where n is a large prime. Let $h \in \langle g \rangle$ denote a random group element such that $\log_g h$ is unknown to anyone.

Consider the following protocol for relation $\{(B; x, y) : B = g^x h^y \ \wedge \ xy = 1\}$:

Prover		Verifier
$u, v, w \in_R \mathbb{Z}_n$ $a \leftarrow g^u h^v$ $b \leftarrow B^v h^w$	$\xrightarrow{a, b}$	
		$c \in_R \mathbb{Z}_n$
	$\xleftarrow{c}$	
$r \leftarrow_n u + cx$ $s \leftarrow_n v + cy$ $t \leftarrow_n w - cy^2$	$\xrightarrow{r, s, t}$	
		$g^r h^s \stackrel{?}{=} aB^c$ $B^s h^t \stackrel{?}{=} bg^c$

a) *Show that the protocol is a Σ-protocol.*

b) *What happens if the challenge is generated as $c = H(a, b)$ (hence omitting B from the input to H) to obtain a non-interactive Σ-proof? Is it secure? Explain your answer.*

1a: 6	1c: 4	2a: 6	3a: 11	4a: 6	homework
1b: 3		2b: 6	3b: 3	4b: 5	min. 0, max. 5

The final mark is the total number of points divided by 5, rounded to a multiple of 0.5, not exceeding 10.

Cryptography 2 (2XC13) / Cryptographic Protocols (2XC10)
Exam, June 27, 2011, 2:00–5:00pm

Solve the following four problems, providing full motivation for the correctness and completeness of your solution.

Use of a simple, non-programmable pocket calculator is allowed, but not necessary. All other electronic equipment is not allowed, nor any notes or books.

Hand in your answer pages, not your scrap paper. GOOD LUCK!

---

1) Let K, M be positive integers with $K \leq M$.

Consider distributions X and Y given by

$$\begin{aligned} X &= \{r + s : r \in_R \{0, \ldots, M-1\}, s \in_R \{0, \ldots, K-1\}\}, \\ Y &= \{u : u \in_R \{0, \ldots, M+K-2\}\}. \end{aligned}$$

Let Δ denote statistical distance.

a) *Determine $\Delta(X, Y)$ for $K = 1$ and arbitrary $M \geq K$.*

b) *Determine $\Delta(X, Y)$ for $K = 2$ and arbitrary $M \geq K$.*

c) *Determine $\Delta(X, Y)$ for $K = 3$ and arbitrary $M \geq K$.*

d) *Determine $\Delta(X, Y)$ for $K = 4$ and arbitrary $M \geq K$.*

e) *Do you think that to obtain a uniform value on $\{0, 1, \ldots, 2M-2\}$ it is a good idea to add two (independent) uniform random values from $\{0, 1, \ldots, M-1\}$?*

2) Let $\langle g \rangle$ be a cyclic group of order n, where n is a large prime.

Consider the following two computational problems:

<u>DH2-invsqm **problem:**</u> given g^x, g^y, compute $g^{x^2 - 1/y^2}$, where $x \in \mathbb{Z}_n$ and $y \in \mathbb{Z}_n^*$.

<u>DH-rec1 **problem:**</u> given g^x, compute $g^{1/(x-1)^2}$, where $x \in \mathbb{Z}_n \setminus \{1\}$.

a) *Show that the* DH2-invsqm *problem is random self-reducible.*

b) *Show that the* DH-rec1 *problem is random self-reducible.*

3) Let $\langle g \rangle$ be a cyclic group of order n, where n is a large prime.

Consider the relation R given by

$$R = \{(A, B, C; x) : A = g^x \ \wedge \ (B = g^{x+x^2} \ \vee \ C = g^{x-x^2})\}.$$

a) *Give a Σ-protocol for relation R and show that it is complete, special sound, and special honest-verifier zero-knowledge.*

b) *Let $\mathcal{H}$ denote a cryptographic hash function. Turn the above Σ-protocol into a non-interactive Σ-proof (using the Fiat-Shamir heuristic) and show how the proof is verified.*

4) Let $\langle g \rangle$ be a cyclic group of order n, where n is a large prime.

Consider the following protocol for relation $\{(h; x) : h = g^x\}$:

Prover		Verifier
$u \in_R \mathbb{Z}_n^*$		
$a \leftarrow g^u$		
$b \in_R \mathbb{Z}_n$	$\xrightarrow{a,\, b}$	
	$\xleftarrow{c}$	$c \in_R \mathbb{Z}_n$
$r \leftarrow_n (b+c)u + x$	$\xrightarrow{r}$	
		$g^r \stackrel{?}{=} a^{b+c}h$

a) *Show that the protocol is complete and special sound.*

b) *Show that the protocol is special honest-verifier zero-knowledge.*

c) *Is the protocol secure against a cheating verifier?*

1a: 1	1c: 3	1e: 3	2a: 6	3a: 10	4a: 4	4c: 3
1b: 2	1d: 4		2b: 6	3b: 3	4b: 5	

The final mark is the total number of points divided by 5, rounded to a multiple of 0.5, not exceeding 10.

Cryptography 2 (2XC13) / Cryptographic Protocols (2XC10)
Exam, April 4, 2011, 2:00–5:00pm

Solve the following four problems, providing full motivation for the correctness and completeness of your solution.

Use of a simple, non-programmable pocket calculator is allowed, but not necessary. All other electronic equipment is not allowed, nor any notes or books.

Hand in your answer pages, not your scrap paper. GOOD LUCK!

---

1) Let K, M be a positive integers with $K < M$. Consider distributions X, Y, Z given by

$$\begin{aligned} X &= \{u : u \in_R \{1, \ldots, KM\}\} \\ Y &= \{uM : u \in_R \{1, \ldots, K\}\} \\ Z &= \{uK : u \in_R \{1, \ldots, M\}\}. \end{aligned}$$

Let Δ denote statistical distance.

a) *Determine* $\Delta(X, Y)$ *and* $\Delta(X, Z)$.

b) *Determine* $\Delta(Y, Z)$ *assuming that* $\gcd(K, M) = 1$.

c) *Determine* $\Delta(Y, Z)$ *for arbitrary positive integers* K, M *with* $K < M$.

2) Let $\langle g \rangle$ be a cyclic group of order n, where n is a large prime.
Consider the following two computational problems:

<u>DH2-3S **problem:**</u> given $(g^x, g^y, g^{(x+y)^2})$, compute $g^{(x+y)^3}$, where $x, y \in \mathbb{Z}_n$;

<u>DH-rat **problem:**</u> given (g^x, g^{x^2}, g^y), compute $(g^{1/x}, g^{y/x})$, where $x \in \mathbb{Z}_n^*$ and $y \in \mathbb{Z}_n$.

a) *Show that the* DH2-3S *problem is random self-reducible.*

b) *Show that the* DH-rat *problem is random self-reducible.*

3) Let $\langle g \rangle$ be a cyclic group of order n, where n is a large prime.

Consider the relation R given by

$$R = \{(A, B, C; x) : A = g^x \ \wedge \ (B = g^{x^2} \ \vee \ C = g^{-x^2})\}.$$

a) *Give a Σ-protocol for relation R and show that it is complete, special sound, and special honest-verifier zero-knowledge.*

b) *Let $\mathcal{H}$ denote a cryptographic hash function. Turn the above Σ-protocol into a non-interactive Σ-proof (using the Fiat-Shamir heuristic) and show how the proof is verified.*

4) Let $\langle g \rangle$ be a cyclic group of order n, where n is a large prime. Consider the following protocol for relation $\{(h_1, h_2; x_1, x_2) : h_1 = g^{x_1}, h_2 = g^{x_2}\}$:

Prover		Verifier
$u \in_R \mathbb{Z}_n$ $a \leftarrow g^u$		
	$\xrightarrow{\quad a \quad}$	
		$c \in_R \mathbb{Z}_n$
	$\xleftarrow{\quad c \quad}$	
$r \leftarrow_n u + cx_1 + c^2 x_2$		
	$\xrightarrow{\quad r \quad}$	
		$g^r \stackrel{?}{=} a h_1^c h_2^{c^2}$

a) *Show that the protocol is complete and special honest-verifier knowledge.*

b) *Why does special soundness not hold for this protocol? Hint: consider a prover who knows $x_1 = \log_g h_1$ but does not know $x_2 = \log_g h_2$.*

c) *Show that soundness holds in the following sense. For any $(h_1, h_2) \in \langle g \rangle \times \langle g \rangle$, given* three *accepting conversations $(a; c; r)$, $(a; c'; r')$, $(a; c''; r'')$ with $c \neq c'$, $c \neq c''$, $c' \neq c''$, show how to efficiently compute witness (x_1, x_2) satisfying $h_1 = g^{x_1}$ and $h_2 = g^{x_2}$.*

1a: 4	1c: 5	2a: 6	3a: 10	4a: 4	4c: 4	homework
1b: 4		2b: 6	3b: 3	4b: 4		min. 0, max. 5

The final mark is the total number of points divided by 5, rounded to a multiple of 0.5, not exceeding 10.

Cryptography 2 (2XC13) / Cryptographic Protocols (2XC10)
Exam, June 28, 2010, 2:00–5:00pm

Solve the following four problems, providing full motivation for the correctness and completeness of your solution.

Use of a simple, non-programmable pocket calculator is allowed, but not necessary. All other electronic equipment is not allowed, nor any notes or books.

Hand in your answer pages, not your scrap paper. GOOD LUCK!

---

1) Let p denote an odd prime. Recall that $\mathbb{Z}_p^* = QR_p \cup \overline{QR_p}$, where

$$QR_p = \{x : \exists_{y \in \mathbb{Z}_p^*}\ x = y^2\}$$

$$\overline{QR_p} = \mathbb{Z}_p^* \setminus QR_p$$

denote the set of quadratic residues modulo p and the set of quadratic nonresidues modulo p, respectively.

Let g denote a generator of $\mathbb{Z}_p^*$, hence $\mathbb{Z}_p^* = \{1, g, g^2, ..., g^{p-2}\}$ and $g^{p-1} = 1$ where all multiplications are modulo p.

Consider distributions X, Y, Z given by

$$\begin{aligned} X &= \{u^2 : u \in_R \mathbb{Z}_p^*\}, \\ Y &= \{g^b u^2 : b \in_R \{0,1\}, u \in_R \mathbb{Z}_p^*\}, \\ Z &= \{g u^2 : u \in_R \mathbb{Z}_p^*\}, \end{aligned}$$

where all multiplications are modulo p.

Let Δ denote statistical distance.

a) *Determine* $\Delta(X, Y)$.

b) *Determine* $\Delta(X, Z)$.

c) *Determine* $\Delta(Y, Z)$.

2) Let $\langle g \rangle$ be a cyclic group of order n, where n is a large prime.
Consider the following two computational problems:

<u>DH-sumsq **problem:**</u> given (g^x, g^y), compute $g^{(x+y)^2}$, where $x, y \in \mathbb{Z}_n$.

<u>DH-4inv2 **problem:**</u> given (g^x, g^y), compute $g^{(1/x^4)+y^2}$, where $x \in \mathbb{Z}_n^*$ and $y \in \mathbb{Z}_n$;

a) *Show that the* DH-sumsq *problem is random self-reducible.*

b) *Show that the* DH-4inv2 *problem is random self-reducible.*

3) Let $\langle g \rangle$ be a cyclic group of order n, where n is a large prime. Further, let $f, h \in \langle g \rangle$ denote random group elements, such that $\log_g f$, $\log_g h$, and $\log_f h$ are unknown to anyone.

Consider the relation R given by

$$R = \{(B; w, x, y) \mid B = f^w g^x h^y \ \wedge \ w + x \in \{1, -1\}\}.$$

a) *Give a Σ-protocol for relation R and show that it is complete, special sound, and special honest-verifier zero-knowledge.*

b) *Let $\mathcal{H}$ denote a cryptographic hash function. Turn the above Σ-protocol into a non-interactive Σ-proof (using the Fiat-Shamir heuristic) and show how the proof is verified.*

4) Let $\langle g \rangle$ be a cyclic group of order n, where n is a large prime.

Consider the following voting scheme, involving voters $V_0, \ldots, V_\ell$, $\ell \geq 1$. Each voter V_i, $0 \leq i < \ell$ has a public key $h_i = g^{x_i}$, where $x_i \in_R \mathbb{Z}_n$ is V_i's private key. (Voter V_ℓ does not need a public key.) Each voter V_i selects a vote $v_i \in \{0, 1\}$, $0 \leq i \leq \ell$.

Let $H_i = \prod_{j=0}^{i} h_j$, for $0 \leq i < \ell$. First, voter V_ℓ publishes an encryption of its vote v_ℓ under public key $H_{\ell-1}$:

$$(a_{\ell-1}, b_{\ell-1}) = (g^{r_\ell}, H_{\ell-1}^{r_\ell} g^{v_\ell}),$$

where $r_\ell \in_R \mathbb{Z}_n$.

For $i = \ell - 1, \ldots, 1$ (in this order), voter V_i publishes the following encryption:

$$(a_{i-1}, b_{i-1}) = (a_i g^{r_i}, b_i a_i^{-x_i} H_{i-1}^{r_i} g^{v_i}),$$

where $r_i \in_R \mathbb{Z}_n$.

Finally, voter V_0 publishes $b_0 a_0^{-x_0} g^{v_0}$.

a) *Let $t_i = \sum_{j=i+1}^{\ell} v_j$, for $0 \leq i < \ell$. Prove (by induction on i) that (a_i, b_i) is an ElGamal encryption of g^{t_i} under public key H_i.*

b) *Show that V_0 outputs $g^{\sum_{j=0}^{\ell} v_j}$.*

c) *Show how $V_0, \ldots, V_i$ are jointly able to decrypt (a_i, b_i), for any i, $1 \leq i < \ell$. Should this be considered a breach of security of the voting scheme?*

d) *Describe the relations that need to be proved by each voter V_i to show that its output is formed correctly. Distinguish the three cases $i = 0$, $0 < i < \ell$, and $i = \ell$, and let each voter use its private values (where applicable) and any publicly available information.*

1a:	4	1c:	4	2a:	6	3a:	10	4a:	5	4c:	3
1b:	4			2b:	6	3b:	3	4b:	2	4d:	3

The final mark is the total number of points divided by 5, rounded to a multiple of 0.5, not exceeding 10.

Cryptography 2 (2XC13) / Cryptographic Protocols (2XC10)
Exam, April 12, 2010, 2:00–5:00pm

Solve the following four problems, providing full motivation for the correctness and completeness of your solution.

Use of a simple, non-programmable pocket calculator is allowed, but not necessary. All other electronic equipment is not allowed, nor any notes or books.

Hand in your answer pages, not your scrap paper. GOOD LUCK!

---

1) Let p denote an odd prime. Recall that $\mathbb{Z}_p^* = QR_p \cup \overline{QR_p}$, where

$$QR_p = \{x : \exists_{y \in \mathbb{Z}_p^*}\ x = y^2\}$$

denotes the set of quadratic residues modulo p and

$$\overline{QR_p} = \mathbb{Z}_p^* \setminus QR_p$$

denotes the set of quadratic nonresidues modulo p.

Let g denote a generator of $\mathbb{Z}_p^*$, hence $\mathbb{Z}_p^* = \{1, g, g^2, ..., g^{p-2}\}$ and $g^{p-1} = 1$ where all multiplications are modulo p.

a) *Express the sets QR_p and $\overline{QR_p}$ in terms of powers of generator g.*

Consider distributions X, Y, Z given by

$$\begin{aligned} X &= \{u : u \in_R \mathbb{Z}_p^*\} \\ Y &= \{u^2 : u \in_R \mathbb{Z}_p^*\} \\ Z &= \{g\ u^2 : u \in_R \mathbb{Z}_p^*\}, \end{aligned}$$

where all multiplications are modulo p.

Let Δ denote statistical distance.

b) *Show that $\Delta(Y, Z) = 1$.*

c) *Show that $\Delta(X, Y) = \Delta(X, Z) = 1/2$.*

2) Let $\langle g \rangle$ be a cyclic group of order n, where n is a large prime.
Consider the following two computational problems:

<u>DH2-3 **problem:**</u> given $(g^x, g^y, g^{x^2}, g^{y^2})$, compute $g^{x^3+y^3}$, where $x, y \in \mathbb{Z}_n$;

<u>DH-pol **problem:**</u> given $(g^x, g^{1/x}, g^y)$, compute $(g^{x^2}, g^{x^2 y})$, where $x \in \mathbb{Z}_n^*$ and $y \in \mathbb{Z}_n$.

a) *Show that the* DH2-3 *problem is random self-reducible.*

b) *Show that the* DH-pol *problem is random self-reducible.*

3) Let $\langle g \rangle$ be a cyclic group of order n, where n is a large prime.

Consider the relation R given by

$$R = \{(A, B, C; x, y, z) : A = g^x \ \wedge \ B = g^y \ \wedge \ C = g^{xyz} \ \wedge \ z \in \{1, -1\}\}.$$

a) *Give a Σ-protocol for relation R and show that it is complete, special sound, and special honest-verifier zero-knowledge.*

b) *Let $\mathcal{H}$ denote a cryptographic hash function. Turn the above Σ-protocol into a non-interactive Σ-proof (using the Fiat-Shamir heuristic) and show how the proof is verified.*

4) Let $\langle g \rangle$ be a cyclic group of order n, where n is a large prime. Consider the following protocol for relation $\{(h_1, h_2; x_1, x_2) : h_1 = g^{x_1}, h_2 = g^{x_2}\}$:

Prover		Verifier
$u \in_R \mathbb{Z}_n$ $a \leftarrow g^u$		
	$\xrightarrow{\quad a \quad}$	
		$c \in_R \mathbb{Z}_n$
	$\xleftarrow{\quad c \quad}$	
$r \leftarrow_n u + cx_1 + c^2 x_2$		
	$\xrightarrow{\quad r \quad}$	
		$g^r \stackrel{?}{=} a h_1^c h_2^{c^2}$

a) *Show that the protocol is complete and special honest-verifier knowledge.*

b) *Why does special soundness not hold for this protocol? Hint: consider a prover who knows $x_1 = \log_g h_1$ but does not know $x_2 = \log_g h_2$.*

c) *Show that soundness holds in the following sense. For any $(h_1, h_2) \in \langle g \rangle \times \langle g \rangle$, given three accepting conversations $(a; c; r)$, $(a; c'; r')$, $(a; c''; r'')$ with $c \neq c'$, $c \neq c''$, $c' \neq c''$, show how to efficiently compute witness (x_1, x_2) satisfying $h_1 = g^{x_1}$ and $h_2 = g^{x_2}$.*

1a: 3	1c: 6	2a: 6	3a: 10	4a: 4	4c: 4	homework
1b: 3		2b: 7	3b: 3	4b: 4		min. 0, max. 5

The final mark is the total number of points divided by 5, rounded to a multiple of 0.5, not exceeding 10.

Cryptography 2 (2XC13) / Cryptographic Protocols (2XC10)
Exam, August 28, 2009, 2:00–5:00pm

Solve the following four problems, providing full motivation for the correctness and completeness of your solution.

Use of a simple, non-programmable pocket calculator is allowed, but not necessary. All other electronic equipment is not allowed, nor any notes or books.

Hand in your answer pages, not your scrap paper. GOOD LUCK!

---

1) Let m be an RSA modulus, hence $m = pq$, where p and q are large, distinct primes of equal bit length k. Recall that $\mathbb{Z}_m^* = \{x \ : \ 0 \leq x < m, \ \gcd(x, m) = 1\}$.

Let U_m denote the uniform distribution on $\mathbb{Z}_m$, and let V_m denote the uniform distribution on $\mathbb{Z}_m^*$.

a) *Determine the statistical distance* $\Delta(U_m, V_m)$.

b) *Suppose a protocol requires a party to use a uniformly random value in* $\mathbb{Z}_m^*$. *Explain whether using a uniformly random value in* $\mathbb{Z}_m$ *instead is good idea or not.*

2) Let $\langle g \rangle$ be a cyclic group of order n, where n is a large prime.
Consider the following two computational problems:

<u>DH-sq2 **problem:**</u> given g^x, g^y, g^{xy}, compute $g^{x^2+y^2}$, where $x, y \in \mathbb{Z}_n$;

<u>DL2-invsq **problem:**</u> given g^x, g^y, compute $g^{(1/x^2)+y^2}$, where $x \in \mathbb{Z}_n^*$ and $y \in \mathbb{Z}_n$.

a) *Show that the* DH-sq2 *problem is random self-reducible.*

b) *Show that the* DL2-invsq *problem is random self-reducible.*

3) Let $\langle g \rangle$ be a cyclic group of order n, where n is a large prime. Further, let $h \in \langle g \rangle$ denote a random group element, such that $\log_g h$ is unknown to anyone.

Consider the relation R given by

$$R = \{(A, B; w, x, y, z) \mid A = g^w h^x \wedge \ B = g^y h^z \ \wedge \ y = wz \ \wedge \ w \in \{0, 1\}\}.$$

a) *Give a* Σ*-protocol for relation* R *and show that it is complete, special sound, and honest-verifier zero-knowledge.*

b) *Let* $\mathcal{H}$ *denote a cryptographic hash function. Turn the above* Σ*-protocol into a non-interactive* Σ*-proof (using the Fiat-Shamir heuristic) and show how the proof is verified.*

4) Let $\langle g \rangle$ be a cyclic group of order n, where n is a large prime. Consider the following Σ-protocol for relation $\{(B; x, y) : B = g^x h^y, \exists_{\chi \in \mathbb{Z}_n} x = \chi^2\}$:

Prover		Verifier
$z, u, v, w \in_R \mathbb{Z}_n$ $A \leftarrow g^\chi h^z$ $a \leftarrow g^u h^v$ $b \leftarrow A^u h^w$		
	$\xrightarrow{A, a, b}$	
		$c \in_R \mathbb{Z}_n$
	$\xleftarrow{c}$	
$r \leftarrow_n u + c\chi$ $s \leftarrow_n v + cz$ $t \leftarrow_n w + c(y - z\chi)$		
	$\xrightarrow{r, s, t}$	
		$g^r h^s \stackrel{?}{=} aA^c$ $A^r h^t \stackrel{?}{=} bB^c$

a) *Show that the protocol is complete, special sound, and honest-verifier knowledge.*

b) *What happens if we generate the challenge as $c = \mathcal{H}(a, b)$ (hence omitting A from the input to $\mathcal{H}$) to obtain a non-interactive version of the protocol? Is it secure? Explain your answer.*

1a: 7	2a: 7	3a: 12	4a: 6
1b: 4	2b: 7	3b: 3	4b: 4

The final mark is the total number of points divided by 5, rounded to a multiple of 0.5, not exceeding 10.

Cryptography 2 (2XC13) / Cryptographic Protocols (2XC10)
Exam, June 15, 2009, 2:00–5:00pm

Solve the following four problems, providing full motivation for the correctness and completeness of your solution.

Use of a simple, non-programmable pocket calculator is allowed, but not necessary. All other electronic equipment is not allowed, nor any notes or books.

Hand in your answer pages, not your scrap paper. GOOD LUCK!

---

1) Let n be an odd prime. Consider distributions X, Y, Z given by:

$$\begin{aligned} X &= \{xy \bmod n : x \in_R \mathbb{Z}_n, y \in_R \mathbb{Z}_n\}, \\ Y &= \{xy \bmod n : x \in_R \mathbb{Z}_n, y \in_R \mathbb{Z}_n^*\}, \\ Z &= \{xy \bmod n : x \in_R \mathbb{Z}_n^*, y \in_R \mathbb{Z}_n^*\}. \end{aligned}$$

Let Δ denote statistical distance.

a) *Determine* $\Delta(X, Y)$ *and* $\Delta(Y, Z)$.

b) *Show that* $\Delta(X, Z) \leq 2/n$.

Let $\langle g \rangle$ be a cyclic group of order n. Define:

$$\begin{aligned} X' &= \{g^{xy} : x \in_R \mathbb{Z}_n, y \in_R \mathbb{Z}_n\}, \\ Z' &= \{g^{xy} : x \in_R \mathbb{Z}_n^*, y \in_R \mathbb{Z}_n^*\}. \end{aligned}$$

c) *Is* $\Delta(X', Z') \leq 2/n$*? Explain your answer.*

2) Let $\langle g \rangle$ be a cyclic group of order n, where n is a large prime.
Consider the following two computational problems:

<u>DH3-inv **problem:**</u> given g^x, g^{x^2}, g^{x^3}, compute $g^{1/x}$, where $x \in \mathbb{Z}_n^*$;

<u>DH3-diffinv **problem:**</u> given $g^x, g^y, g^{1/z}$, compute $g^{(x-y)/z}$, where $x, y \in \mathbb{Z}_n$, $z \in \mathbb{Z}_n^*$.

a) *Show that the* DH3-inv *problem is random self-reducible.*

b) *Show that the* DH3-diffinv *problem is random self-reducible.*

3) Let $\langle g \rangle$ be a cyclic group of order n, where n is a large prime. Further, let $h \in \langle g \rangle$ denote a random group element, such that $\log_g h$ is unknown to anyone.

Consider the relation R given by

$$R = \{(A, B; w, x, y, z) \mid A = g^w h^x \wedge \ B = g^y h^z \ \wedge \ y = wz \ \wedge \ w \in \{1, -1\}\}.$$

a) *Give a Σ-protocol for relation R and show that it is complete, special sound, and honest-verifier zero-knowledge.*

b) *Let $\mathcal{H}$ denote a cryptographic hash function. Turn the above Σ-protocol into a non-interactive Σ-proof (using the Fiat-Shamir heuristic) and show how the proof is verified.*

4) Let $\langle g \rangle$ be a cyclic group of order n, where n is a large prime. Consider the following Σ-protocol for relation $\{(B; x, y) : B = g^x h^y, \exists_{\chi \in \mathbb{Z}_n} x = \chi^2\}$:

Prover		Verifier
$z, u, v, w \in_R \mathbb{Z}_n$ $A \leftarrow g^\chi h^z$ $a \leftarrow g^u h^v$ $b \leftarrow A^u h^w$		
	$\xrightarrow{A, a, b}$	
		$c \in_R \mathbb{Z}_n$
	$\xleftarrow{c}$	
$r \leftarrow_n u + c\chi$ $s \leftarrow_n v + cz$ $t \leftarrow_n w + c(y - z\chi)$		
	$\xrightarrow{r, s, t}$	
		$g^r h^s \stackrel{?}{=} aA^c$ $A^r h^t \stackrel{?}{=} bB^c$

a) *Show that the protocol is complete, special sound, and honest-verifier knowledge.*

b) *What happens if we generate the challenge as $c = \mathcal{H}(a, b)$ (hence omitting A from the input to $\mathcal{H}$) to obtain a non-interactive version of the protocol? Is it secure? Explain your answer.*

1a: 6	1c: 3	2a: 6	3a: 11	4a: 6	homework
1b: 5		2b: 6	3b: 3	4b: 4	min. 0, max. 5

The final mark is the total number of points divided by 5, rounded to a multiple of 0.5, not exceeding 10.

Cryptography 2 (2XC13) / Cryptographic Protocols (2XC10)
Exam, June 23, 2008, 2:00–5:00pm

Solve the following four problems, providing full motivation for the correctness and completeness of your solution.

Use of a simple, non-programmable pocket calculator is allowed, but not necessary. All other electronic equipment is not allowed, nor any notes or books.

Hand in your answer pages, not your scrap paper. GOOD LUCK!

---

1) Let k be a positive integer, and let n be an odd prime with $n < 2^k$. Consider:

$$\begin{aligned} U_n &= \{x \mid x \in_R \mathbb{Z}_n\}, \\ V_{n,k} &= \{x \bmod n \mid x \in_R \{0, \ldots, 2^k - 1\}\}. \end{aligned}$$

Let Δ denote statistical distance.

a) *Show that* $\Delta(U_n, V_{n,k}) = \frac{(2^k \bmod n)(n-(2^k \bmod n))}{2^k n}$.

b) *Show that* $\Delta(U_n, V_{n,k}) \leq n/2^k$.

Suppose k random bits $x_0 \in_R \{0,1\}, \ldots, x_{k-1} \in_R \{0,1\}$ are used to generate a random value modulo n by returning $(\sum_{i=0}^{k-1} x_i 2^i) \bmod n$ as output.

c) *Suggest a value for k as a function of n such that the resulting value is approximately uniformly distributed in $\mathbb{Z}_n$.*

2) Let $\langle g \rangle$ and $\langle G \rangle$ be two, different, cyclic groups both of order n, where n is a large prime. The DL problem is assumed to be hard for both groups. Suppose that a function $S : \langle g \rangle \to \langle G \rangle$ is given satisfying:

$$S(g^x) = G^{x^2}, \quad \text{for all } x \in \mathbb{Z}_n,$$

and that S can be computed efficiently.

We consider a generalization of Diffie-Hellman key exchange with three parties A, B, and C. Party A picks $x_A \in_R \mathbb{Z}_n$ and sends g^{x_A} to parties B and C. Similarly, party B picks $x_B \in_R \mathbb{Z}_n$ and sends g^{x_B} to parties A and C, and party C picks $x_C \in_R \mathbb{Z}_n$ and sends g^{x_C} to parties A and B.

a) *Show how each party can compute the common key $K = G^{x_A x_B x_C}$.*

b) *Show that the DDH problem is easy for the group $\langle g \rangle$.*

Consider the following computational problem:

<u>DH3 **problem:**</u> given g^x, g^y, g^z, compute G^{xyz}, where $x, y, z \in \mathbb{Z}_n$.

c) *Show that the* DH3 *problem is random self-reducible.*

Finally, we consider active attacks for the above key exchange protocol. The attacker can intercept and modify all traffic between parties A, B, C, and its goal is to know all of the keys that parties A, B, C will hold once the key exchange protocol is completed.

d) *Show a man-in-the-middle attack for the above key exchange protocol.*

3) Let $\langle g \rangle$ be a cyclic group of order n, where n is a large prime. Further, let $f, h \in \langle g \rangle$ denote random group elements, such that $\log_g f$, $\log_g h$, and $\log_f h$ are unknown to anyone.

Consider the relation R given by

$$R = \{(A, B; x, y) \mid A = f^x \wedge \ B = g^x h^y \ \wedge \ x^2 = y^2\}\}.$$

a) *Give a Σ-protocol for relation R and show that it is complete, special sound, and honest-verifier zero-knowledge. Hint: first solve the equation $x^2 = y^2 \pmod{n}$.*

b) *Let $\mathcal{H}$ denote a cryptographic hash function. Turn the above Σ-protocol into a non-interactive Σ-proof (using the Fiat-Shamir heuristic) and show how the proof is verified.*

4) Let $\langle g \rangle$ be a cyclic group of order n, where n is a large prime. Consider the following variant of Schnorr's protocol, where $F : \langle g \rangle \to \mathbb{Z}_n$ denotes an arbitrary function:

Prover		Verifier
$(x = \log_g h)$		
$u \in_R \mathbb{Z}_n^*$		
$a \leftarrow g^u$	$\xrightarrow{a}$	
	$\xleftarrow{c}$	$c \in_R \mathbb{Z}_n$
$r \leftarrow_n (c - F(a))u + x$	$\xrightarrow{r}$	
		$g^r \stackrel{?}{=} a^{c-F(a)} h$

a) *Show that the protocol is complete, special sound, and honest-verifier knowledge.*

b) *What happens if we generate the challenge as $c = F(a)$ to obtain a non-interactive version of the protocol?*

1a:	7	1c:	2	2a:	4	2c:	4	3a:	11	4a:	7
1b:	2			2b:	3	2d:	3	3b:	3	4b:	4

The final mark is the total number of points divided by 5, rounded to a multiple of 0.5.

Cryptography 2 (2XC13) / Cryptographic Protocols (2XC10) Exam, April 28, 2008, 2:00–5:00pm

---

Solve the following four problems, providing full motivation for the correctness and completeness of your solution.

Use of a simple, non-programmable pocket calculator is allowed, but not necessary. All other electronic equipment is not allowed, nor any notes or books.

Hand in your answer pages, not your scrap paper. GOOD LUCK!

---

1) Let M and K be positive integers, $M \leq K$. Consider distributions V_m, $0 \leq m < M$, given by

$$V_m = \{m + r \mid r \in_R \{0, \ldots, K-1\}\}.$$

Let Δ denote statistical distance.

a) *Determine $\Delta(V_m, V_{m'})$ for any $m, m' \in \{0, \ldots, M-1\}$.*

Consider the following $(2,2)$-threshold secret sharing scheme. The dealer holds a secret $s \in \{0, ..., M-1\}$. The dealer picks $r \in_R \{0, \ldots, K-1\}$ and sets share $s_1 = s + r$ and $s_2 = r$. The secret is recovered by computing $s = s_1 - s_2$.

b) *Propose a value for K as a function of M and argue why the secret sharing scheme is secure (against passive attacks).*

2) Let $\langle g \rangle$ and $\langle G \rangle$ be two, different, cyclic groups both of order n, where n is a large prime. The DL problem is assumed to be hard for both groups. Suppose that a function $P : \langle g \rangle \times \langle g \rangle \to \langle G \rangle$ is given satisfying:

$$P(g^x, g^y) = G^{xy}, \quad \text{for all } x, y \in \mathbb{Z}_n,$$

and that P can be computed efficiently.

We consider a generalization of Diffie-Hellman key exchange with three parties A, B, and C. Party A picks $x_A \in_R \mathbb{Z}_n$ and sends g^{x_A} to parties B and C. Similarly, party B picks $x_B \in_R \mathbb{Z}_n$ and sends g^{x_B} to parties A and C, and party C picks $x_C \in_R \mathbb{Z}_n$ and sends g^{x_C} to parties A and B.

a) *Show how each party can compute the common key $K = G^{x_A x_B x_C}$.*

b) *Show that the DDH problem is easy for the group $\langle g \rangle$.*

Consider the following two computational problems:

<u>DH3* **problem:**</u> given g^x, g^y, g^z, compute G^{xyz}, where $x, y, z \in \mathbb{Z}_n^*$;

<u>DH3 **problem:**</u> given g^x, g^y, g^z, compute G^{xyz}, where $x, y, z \in \mathbb{Z}_n$.

c) *Show that the* DH3* *problem is random self-reducible.*

d) *Show that the* DH3 *problem is random self-reducible.*

Finally, we consider active attacks for the above key exchange protocol. The attacker can intercept and modify all traffic between parties A, B, C, and its goal is to know all of the keys that parties A, B, C will hold once the key exchange protocol is completed.

e) *Show a man-in-the-middle attack for the above key exchange protocol.*

3) Let $\langle g \rangle$ be a cyclic group of order n, where n is a large prime. Further, let $f, h \in \langle g \rangle$ denote random group elements, such that $\log_g f$, $\log_g h$, and $\log_f h$ are unknown to anyone.

Consider the relation R given by

$$R = \{(B; w, x, y) \mid B = f^w g^x h^y \ \wedge \ w - x \in \{0, 1\}\}.$$

a) *Give a Σ-protocol for relation R and show that it is complete, special sound, and honest-verifier zero-knowledge.*

b) *Let $\mathcal{H}$ denote a cryptographic hash function. Turn the above Σ-protocol into a non-interactive Σ-proof (using the Fiat-Shamir heuristic) and show how the proof is verified.*

4) Let $\langle g \rangle$ be a cyclic group of order n, where n is a large prime.

Consider the following basic idea for constructing an (ℓ, ℓ)-threshold Schnorr signature scheme. Suppose parties P_i each hold a private key x_i and a public key $h_i = g^{x_i}$, for $1 \leq i \leq \ell$. Define $h = \prod_{i=1}^{\ell} h_i$ as the public key of parties $P_1, \ldots, P_\ell$ together.

For a given message m, the goal is to jointly generate a Schnorr signature (c, r) for public key h, where $c = \mathcal{H}(g^r h^{-c}, m)$. Suppose party P_0 acts as a 'combiner', acting as the verifier in a run of the Schnorr protocol with each of the parties P_i.

a) *Show how P_0 can generate a Schnorr signature (c, r) for public key h, by running the Schnorr protocol ℓ times in parallel, once with each party P_i for public key h_i (P_i acting as the prover, P_0 as the verifier). Argue why the scheme is secure.*
Hint: how should P_0 choose the challenges c_i such that the conversations (a_i, c_i, r_i) of the runs of the Schnorr protocol can be combined?

b) *Describe how your scheme can be extended to a (t, ℓ)-threshold Schnorr signature scheme, $1 \leq t \leq \ell$. You may assume that the parties have already run a distributed key generation protocol such that P_i holds a share x_i, where $x_i = f(i)$ for some polynomial f of degree $< t$, and $x = f(0)$. As before, the public key of party P_i is $h_i = g^{x_i}$.*
Hint: how do you compute the public key $h = g^x$ from $h_1, \ldots, h_\ell$?

1a: 5	2a: 3	2c: 5	2e: 4	3a: 10	4a: 4	homework
1b: 3	2b: 4	2d: 5		3b: 3	4b: 4	min. 0, max. 5

The final mark is the total number of points divided by 5, rounded to a multiple of 0.5, not exceeding 10.

Cryptography 2 (2WC13) / Cryptographic Protocols (2WC10)
Exam, July 6, 2007, 2:00–5:00pm

Solve the following problems, providing full motivation for the correctness and completeness of your solution.

Use of a simple, non-programmable pocket calculator is allowed, but not necessary. All other electronic equipment is not allowed, nor any notes or books.

Hand in your answer pages, not your scrap paper. GOOD LUCK!

---

1) Let m be a positive integer. Consider distributions X, Y, Z given by

$$\begin{aligned} X &= \{x \mid x \in_R \{0, \ldots, m-1\}\} \\ Y &= \{2x \mid x \in_R \{0, \ldots, m-1\}\} \\ Z &= \{2x+1 \mid x \in_R \{0, \ldots, m-1\}\}. \end{aligned}$$

Let Δ denote statistical distance.

a) *Show that* $\Delta(Y, Z) = 1$.

b) *Show that* $\Delta(X, Y) = \Delta(X, Z) = 1/2$ *for even* m.

c) *Also determine* $\Delta(X, Y)$ *and* $\Delta(X, Z)$ *for odd* m.

2) Let $\langle g \rangle$ be a cyclic group of order n, where n is a large prime.
Consider the following two computational problems:

<u>DH3-sym **problem:**</u> given g^x, g^y, g^z, compute $g^{xy+yz+zx}$, where $x, y, z \in \mathbb{Z}_n$;

<u>DH3-suminv **problem:**</u> given $g^x, g^y, g^{1/z}$, compute $g^{(x+y)/z}$, where $x, y \in \mathbb{Z}_n$, $z \in \mathbb{Z}_n^*$.

a) *Show that the* DH3-sym *problem is random self-reducible.*

b) *Show that the* DH3-suminv *problem is random self-reducible.*

3) Let $\langle g \rangle$ be a cyclic group of order n, where n is a large prime. Further, let $h \in \langle g \rangle$ denote a random group element, such that $\log_g h$ is unknown to anyone.

Consider the relation R given by

$$R = \{(A, B; x, y) \mid A = g^x \ \wedge \ B = h^y \ \wedge \ x^2 = y^2\}.$$

a) *Give a* Σ*-protocol for relation* R *and show that it is complete, special sound, and honest-verifier zero-knowledge. (Hint: first solve the equation* $x^2 = y^2 \pmod{n}$*.)*

b) *Let* $\mathcal{H}$ *denote a cryptographic hash function. Turn the above* Σ*-protocol into a non-interactive* Σ*-proof (using the Fiat-Shamir heuristic) and show how the proof is verified.*

4) Let $\langle g \rangle$ be a cyclic group of order n, where n is a large prime. Further, let $h \in \langle g \rangle$ denote a random group element, such that $\log_g h$ is unknown to anyone.

Consider the following protocol:

Prover		Verifier
$(B = g^x h^y)$		
$u, v \in_R \mathbb{Z}_n$ $a \leftarrow g^u$ $b \leftarrow h^v$		
	$\xrightarrow{a,\, b}$	
		$c \in_R \mathbb{Z}_n$
	$\xleftarrow{c}$	
$r \leftarrow_n u + cx$ $s \leftarrow_n v + cy$		
	$\xrightarrow{r,\, s}$	
		$g^r h^s \stackrel{?}{=} abB^c$

a) *Verify that the protocol is complete and special sound for the relation R given by*

$$R = \{(B; x, y) \mid B = g^x h^y\}.$$

b) *Is the protocol honest-verifier zeroknowledge for relation R? If yes, give a simulation; if no, show what information leaks.*

5) Consider the following basic idea for constructing a (t, ℓ)-threshold cryptosystem from a given public key cryptosystem with message space $\mathbb{Z}_n$, for a prime n.

Each party P_i, $1 \leq i \leq \ell$, generates its own key pair consisting of a private key and a public key for the basic public key cryptosystem, and all these public keys are made public. To encrypt a message $m \in \mathbb{Z}_n$, one first splits m into shares $m_1, \ldots, m_\ell$ as in the distribution protocol of Shamir's (t, ℓ)-threshold scheme (using m as the secret). Then one encrypts one share for each party. All encryptions together form a ciphertext. For decryption, a sufficient number of shares need to be decrypted to be able to reconstruct message m from it (hence t or more parties must use their private key).

a) *Give a full description of such a (t, ℓ)-threshold cryptosystem, specifying the exact steps for the Distributed Key Generation protocol, for the Encryption algorithm and for the Threshold Decryption protocol.*

b) *Discuss the security of this threshold cryptosystem.*

1a: 2	1c: 4	2a: 5	3a: 9	4a: 4	5a: 4
1b: 6		2b: 5	3b: 2	4b: 5	5b: 4

The final mark is the total number of points divided by 5, rounded to a multiple of 0.5, but not exceeding 10.

Cryptographic Protocols (2WC01) / Cryptography 2 (2WC13)
Exam, May 9, 2007, 2:00–5:00pm

Solve the following problems, providing full motivation for the correctness and completeness of your solution.

Use of a simple, non-programmable pocket calculator is allowed, but not necessary. All other electronic equipment is not allowed, nor any notes or books.

Hand in your answer pages, not your scrap paper. GOOD LUCK!

1) Consider the following protocol for transferring a message $m \in \{0, 1, \ldots, 2^{16} - 1\}$ from party A to party B, where $k \geq 0$ is a security parameter. The object of the protocol is to hide message m from other parties than A and B.

Party A		Party B
$u_A \in_R \{0, \ldots, 2^k - 1\}$		$u_B \in_R \{0, \ldots, 2^k - 1\}$
$c_A \leftarrow m + u_A$	$\xrightarrow{c_A}$	
	$\xleftarrow{c_{AB}}$	$c_{AB} \leftarrow c_A + u_B$
$c_B \leftarrow c_{AB} - u_A$	$\xrightarrow{c_B}$	$m' \leftarrow c_B - u_B$

Note that c_A, c_{AB}, c_B and m' are computed using addition and subtraction are over $\mathbb{Z}$.

a) *Verify that $m' = m$ if A and B follow the protocol.*

Next, consider distributions U and V_m, given by

$$\begin{aligned} U &= \{u \mid u \in_R \{0, \ldots, 2^k - 1\}\}, \text{ and} \\ V_m &= \{m + u \mid u \in_R \{0, \ldots, 2^k - 1\}\}. \end{aligned}$$

b) *Compute the statistical distance $\Delta(U, V_m)$ as a function of m and k.*

c) *Prove that $\Delta(V_m, V_n) \leq (m + n)/2^k$ for any $m, n \in \{0, 1, \ldots, 2^{16} - 1\}$, using the triangle inequality for Δ. Is this upper bound tight?*

d) *Suppose that we want a passive attacker who only knows c_A to be able to guess the value for m with probability at most 2^{-80}. What value should we set for k approximately? Is the protocol also secure against an arbitrary passive attacker?*

2) Let $\langle g \rangle$ be a cyclic group of order n, where n is a large prime.
Consider the following two computational problems:

<u>DH-INV **problem:**</u> given g^x, g^y, g^{xy}, compute $g^{1/(xy)}$, where $x, y \in \mathbb{Z}_n^* = \mathbb{Z}_n \setminus \{0\}$;

<u>DH-INV+ **problem:**</u> given g^x, g^y, g^{xy}, compute $g^{(1/x)+y}$, where $x \in \mathbb{Z}_n^*$ and $y \in \mathbb{Z}_n$.

a) *Show that the* DH-INV *problem is random self-reducible.*

b) *Show that the* DH-INV+ *problem is random self-reducible.*

3) Let $\langle g \rangle$ be a cyclic group of order n, where n is a large prime. Further, let $f, h \in \langle g \rangle$ denote random group elements, such that $\log_g f$, $\log_g h$ and $\log_f h$ are unknown to anyone.

Consider the relation R given by

$$R = \{(B; w, x, y) \mid B = f^w g^x h^y \ \wedge \ (w = x \ \vee \ x = y)\}.$$

a) *Give a Σ-protocol for relation R and show that it is complete, special sound, and honest-verifier zero-knowledge.*

b) *Let $\mathcal{H}$ denote a cryptographic hash function. Turn the above Σ-protocol into a non-interactive Σ-proof (using the Fiat-Shamir heuristic) and show how the proof is verified.*

4) Let $\langle g \rangle$ be a cyclic group of order n, where n is a large prime.

Consider the following basic idea for constructing an (ℓ, ℓ)-threshold Schnorr signature scheme. Suppose parties P_i each hold a private key x_i and a public key $h_i = g^{x_i}$, for $1 \leq i \leq \ell$. Define $h = \prod_{i=1}^{\ell} h_i$ as the public key of parties $P_1, \ldots, P_\ell$ together.

For a given message m, the goal is to jointly generate a Schnorr signature (c, r) for public key h, where $c = \mathcal{H}(g^r h^{-c}, m)$. Suppose party P_0 acts as a 'combiner', acting as the verifier in a run of the Schnorr protocol with each of the parties P_i.

a) *Show how P_0 can generate a Schnorr signature (c, r) for public key h, by running the Schnorr protocol ℓ times in parallel, once with each party P_i for public key h_i (P_i acting as the prover, P_0 as the verifier). Argue why the scheme is secure.*
Hint: how should P_0 choose the challenges c_i such that the conversations (a_i, c_i, r_i) of the runs of the Schnorr protocol can be combined?

b) *Describe how your scheme can be extended to a (t, ℓ)-threshold Schnorr signature scheme, $1 \leq t \leq \ell$. You may assume that the parties have already run a distributed key generation protocol such that P_i holds a share x_i, where $x_i = f(i)$ for some polynomial f of degree $< t$, and $x = f(0)$. As before, the public key of party P_i is $h_i = g^{x_i}$.*
Hint: how do you compute the public key $h = g^x$ from $h_1, \ldots, h_\ell$?

1a:	2	1c:	4	2a:	6	3a:	10	4a:	6	homework	
1b:	5	1d:	4	2b:	6	3b:	3	4b:	4	min. 0, max. 5	

The final mark is the total number of points divided by 5, rounded to an integer value (for 2WC01) and rounded to a multiple of 0.5 (for 2WC13), but not exceeding 10.

Cryptographic Protocols (2WC01)
Exam, March 19, 2007, 9:00–12:00am

Solve the following problems, providing full motivation for the correctness and completeness of your solution.

Use of a simple, non-programmable pocket calculator is allowed, but not necessary. All other electronic equipment is not allowed.

Hand in your answer pages, not your scrap paper. GOOD LUCK!

---

1) Let $\langle g \rangle$ be a cyclic group of order n, where n is a large prime. Consider the following two protocols between parties A and B connected by an insecure communication channel: Protocol I for sending a message $m \in \langle g \rangle$, $m \neq 1$, securely from party A to party B, and Protocol II for sending a message $b \in \{0, 1\}$, securely from party A to party B (with $\oplus$ denoting exclusive-or).

Protocol I

Party A		Party B
$x_A \in_R \mathbb{Z}_n^*$		
$y_A \leftarrow m^{x_A}$	$\xrightarrow{y_A}$	
		$x_B \in_R \mathbb{Z}_n^*$
	$\xleftarrow{y_{AB}}$	$y_{AB} \leftarrow y_A^{x_B}$
$y_B \leftarrow y_{AB}^{1/x_A}$		
	$\xrightarrow{y_B}$	
		$m' \leftarrow y_B^{1/x_B}$

Protocol II

Party A		Party B
$b_A \in_R \{0, 1\}$		
$c_A \leftarrow b \oplus b_A$	$\xrightarrow{c_A}$	
		$b_B \in_R \{0, 1\}$
	$\xleftarrow{c_{AB}}$	$c_{AB} \leftarrow c_A \oplus b_B$
$c_B \leftarrow c_{AB} \oplus b_A$		
	$\xrightarrow{c_B}$	
		$b' \leftarrow c_B \oplus b_B$

The object of both protocols is that the message sent remains completely hidden for other parties than A and B, and that the message cannot be modified by other parties than A or B.

a) *Verify that $m' = m$ and $b' = b$ if A and B follow protocols I and II, respectively.*

b) *Compute the statistical distance between $\{u \mid u \in_R \mathbb{Z}_n\}$ and $\{u \mid u \in_R \mathbb{Z}_n^*\}$. Now, does it matter if party B decides to generate $x_B \in_R \mathbb{Z}_n$ instead of $x_B \in_R \mathbb{Z}_n^*$?*

Next, answer the following questions with 'yes' or 'no'; in case of a 'yes' describe the relevant computational assumption (if any), in case of a 'no' show an attack.

c) *Is protocol I secure against* **passive** *attacks?*

d) *Is protocol I secure against* **active** *attacks?*

e) *Is protocol II secure against* **passive** *attacks?*

f) *Is protocol II secure against* **active** *attacks?*

2) Let $\langle g \rangle$ be a cyclic group of order n, where n is a large prime.
Consider the following two computational problems:

<u>DL-INV3 **problem:**</u> given g^x, g^{x^2}, g^{x^3}, compute $g^{1/x}$, where $x \in \mathbb{Z}_n^* = \mathbb{Z}_n \setminus \{0\}$;

<u>DH3 **problem:**</u> given g^x, g^y, g^z, compute $g^{(x+y)z}$, where $x, y, z \in \mathbb{Z}_n$.

a) *Show that the* DL-INV3 *problem is random self-reducible.*

b) *Show that the* DH3 *problem is random self-reducible.*

3) Let $\langle g \rangle$ be a cyclic group of order n, where n is a large prime. Further, let $h \in \langle g \rangle$ denote a random group element, such that $\log_g h$ is unknown to anyone.

Consider the relation R given by

$$R = \{(B; x, y) \mid B = g^x h^y \ \wedge \ (x = 0 \ \vee \ y = 0 \ \vee \ x = y)\}.$$

a) *Give a Σ-protocol for relation R and show that it is complete, special sound, and honest-verifier zero-knowledge.*

b) *Let $\mathcal{H}$ denote a cryptographic hash function. Turn the above Σ-protocol into a non-interactive Σ-proof (using the Fiat-Shamir heuristic) and show how the proof is verified.*

4) Recall Shamir's (t, ℓ)-threshold secret sharing scheme, $1 \leq t \leq \ell$, for sharing a secret by a dealer among participants $P_1, \ldots, P_\ell$ such that any set of t (or more) participants is able to recover the (unique) secret, but any set of $t - 1$ (or less) participants is not able to find any information on the secret. Assume that the scheme is used for secrets belonging to $\mathbb{Z}_p$ for a prime p, where $p > \ell$.

Note that Shamir's scheme only protects against *passive* attacks.

a) *Show how the dealer can mount an* active *attack by deviating from the distribution protocol such that the secret recovered will not be independent of the particular set of t participants taking part in the reconstruction protocol.*

b) *Let s be the value of the secret corresponding to the shares as distributed among the participants by an honest dealer. Suppose that participants $P_1, \ldots, P_t$ decide to recover the secret by combining their shares. Show how participant P_1 can mount an* active *attack by deviating from the reconstruction protocol such that an arbitrary given value $\Delta s \in \mathbb{Z}_p$ will be added to the result (yielding $s + \Delta s \pmod p$) as reconstructed value for the secret).*

1a:	1	1c:	3	1e:	3	2a:	5	3a:	11	4a:	5
1b:	2	1d:	3	1f:	3	2b:	5	3b:	4	4b:	5

The final mark is the total number of points divided by 5, rounded to the nearest integer.

Cryptographic Protocols (2WC01)
Exam, May 11, 2006, 9:00–12:00am

Solve the following problems, providing full motivation for the correctness and completeness of your solution.

Use of a simple, non-programmable pocket calculator is allowed, but not necessary. All other electronic equipment is not allowed.

Hand in your answer pages, not your scrap paper. GOOD LUCK!

---

1) Let m be an RSA modulus, hence $m = pq$, where p and q are large, distinct primes of equal bit length k. Recall that $\mathbb{Z}_m^* = \{x \ : \ 0 \leq x < m, \ \gcd(x, m) = 1\}$ is a set of integers co-prime with m, and that $|\mathbb{Z}_m^*| = \phi(m) = (p-1)(q-1)$.

Let U_m denote the uniform distribution on $\mathbb{Z}_m$, and let V_m denote the uniform distribution on $\mathbb{Z}_m^*$.

a) *Determine the statistical distance* $\Delta(U_m, V_m)$.

b) *Suppose a protocol requires a party to use a uniformly random value in* $\mathbb{Z}_m^*$. *Explain whether using a uniformly random value in* $\mathbb{Z}_m$ *instead is good idea or not.*

Next, let integer $e > 1$ satisfy $\gcd(e, \phi(m)) = 1$. The RSA problem is to compute $x = y^{1/e} \bmod m$, given $y \in \mathbb{Z}_m^*$.

c) *Show that the RSA problem is random self-reducible. Also, explain why the reduction is polynomial time (as a function of the security parameter* k*) and why it is correct.*

2) Let $\langle g \rangle$ be a cyclic group of order n, where n is a large prime. Furthermore, let $E, D : \{0,1\}^* \times \langle g \rangle \to \langle g \rangle$ denote the encryption and decryption algorithms of a symmetric cryptosystem, respectively, such that for any $s \in \{0,1\}^*$ and for any $y \in \langle g \rangle$, we have that $D_s(E_s(y)) = y$. The symmetric cryptosystem is assumed to be secure.

Let $pw \in \{0,1\}^*$ denote a password, which is known to parties A and B only. Consider the following password-based authenticated key exchange protocol:

Party A		Party B
$x_A \in_R \mathbb{Z}_n$		$x_B \in_R \mathbb{Z}_n$
$y_A \leftarrow g^{x_A}$		$y_B \leftarrow g^{x_B}$
$c_A \leftarrow E_{pw}(y_A)$		$c_B \leftarrow E_{pw}(y_B)$
	$\xrightarrow{c_A}$	
	$\xleftarrow{c_B}$	
$K_A \leftarrow (D_{pw}(c_B))^{x_A}$		$K_B \leftarrow (D_{pw}(c_A))^{x_B}$

a) *Show that $K_A = K_B$ if the parties follow the protocol.*

b) *Explain why a passive attacker (eavesdropper) cannot find pw nor K, where $K = K_A = K_B$. Also, explain which computational assumption is needed.*

Next, suppose parties A and B want to confirm to each other that they got the same key K. To this end, A sends to B the ciphertext $E_{pw}(K_A)$ and B sends to A the ciphertext $E_{pw}(K_B)$, after running the above protocol.

c) *Again, explain why a passive attacker (eavesdropper) cannot find pw nor K. Also, explain which computational assumption is needed in this case.*

3) Let $\langle g \rangle$ be a cyclic group of order n, where n is a large prime. Further, let $h \in \langle g \rangle$ denote a random group element, such that $\log_g h$ is unknown to anyone.

Consider the relation R given by

$$R = \{(B; x, y) \mid B = g^x h^y \ \wedge \ (x = 0 \ \vee \ x = y)\}.$$

a) *Give a Σ-protocol for relation R and show that it is complete, special sound, and honest-verifier zero-knowledge.*

b) *Let $\mathcal{H}$ denote a cryptographic hash function. Turn the above Σ-protocol into a non-interactive Σ-proof (using the Fiat-Shamir heuristic) and show how the proof is verified.*

4) Consider the following basic idea for constructing a (t, ℓ)-threshold cryptosystem from a given public key cryptosystem with message space $\mathbb{Z}_n$, for a prime n. Each party P_i, $1 \leq i \leq \ell$, generates its own key pair consisting of a private key and a public key for the basic public key cryptosystem, and all these public keys are made public. To encrypt a message $m \in \mathbb{Z}_n$, one first splits m into shares $m_1, \ldots, m_\ell$ as in the distribution protocol of Shamir's (t, ℓ)-threshold scheme (using m as the secret). Then one encrypts one share for each party. All encryptions together form a ciphertext. For decryption, a sufficient number of shares need to be decrypted to be able to reconstruct message m from it (hence t or more parties must use their private key).

a) *Give a full description of such a (t, ℓ)-threshold cryptosystem, specifying the exact steps for the Distributed Key Generation protocol, for the Encryption algorithm and for the Threshold Decryption protocol.*

b) *Argue why the scheme is secure.*

1a: 7	1c: 7	2a: 2	2c: 5	3a: 10	4a: 4	homework
1b: 3		2b: 5		3b: 4	4b: 3	min. 0, max. 5

The final mark is the total number of points divided by 5, rounded to the nearest integer, but not exceeding 10.

Cryptographic Protocols (2WC01)
Exam, March 20, 2006, 9:00–12:00am

Solve the following problems, providing full motivation for the correctness and completeness of your solution.

Use of a simple, non-programmable pocket calculator is allowed, but not necessary. All other electronic equipment is not allowed.

Hand in your answer pages, not your scrap paper. GOOD LUCK!

---

1) Consider the following protocol for transferring a message $b \in \{0,1\}$ from party A to party B, where $k \geq 0$ is a security parameter. The object of the protocol is to hide message b from other parties than A and B.

Party A		Party B
$u_A \in_R \{0,\ldots,2^k-1\}$		$u_B \in_R \{0,\ldots,2^k-1\}$
$c_A \leftarrow b + u_A$	$\xrightarrow{c_A}$	
	$\xleftarrow{c_{AB}}$	$c_{AB} \leftarrow c_A + u_B$
$c_B \leftarrow c_{AB} - u_A$	$\xrightarrow{c_B}$	$b' \leftarrow c_B - u_B$

Note that c_A, c_{AB}, c_B and b' are computed using addition and subtraction are over $\mathbb{Z}$.

a) *Verify that $b' = b$ if A and B follow the protocol.*

Next, consider distributions U_k and V_k, $k \geq 0$, given by

$$\begin{aligned} U_k &= \{u \mid u \in_R \{0,\ldots,2^k-1\}\}, \text{ and} \\ V_k &= \{u+1 \mid u \in_R \{0,\ldots,2^k-1\}\}. \end{aligned}$$

b) *Compute the statistical distance $\Delta(U_k, V_k)$ as a function of k.*

Finally, suppose k is set such that $\Delta(U_k, V_k) \leq 2^{-80}$. Answer the following questions with 'yes' or 'no', and explain your answer.

c) *Is the protocol secure against a passive attacker who only knows c_A?*

d) *Is the protocol secure against a passive attacker who knows c_A, c_{AB}, and c_B?*

2) Let $\langle g \rangle$ be a cyclic group of order n, where n is a large prime.
Consider the following two computational problems:

<u>DL-INV **problem:**</u> given g^x, compute $g^{1/x}$, where $x \in \mathbb{Z}_n^* = \mathbb{Z}_n \setminus \{0\}$;

<u>DL-SQ2 **problem:**</u> given g^x, g^y, compute $g^{x^2+y^2}$, where $x, y \in \mathbb{Z}_n$.

a) *Show that the* DL-INV *problem is random self-reducible.*

b) *Show that the* DL-SQ2 *problem is random self-reducible.*

3) Let $\langle g \rangle$ be a cyclic group of order n, where n is a large prime. Further, let $h \in \langle g \rangle$ denote a random group element, such that $\log_g h$ is unknown to anyone.

Consider the relation R given by

$$R = \{(h_0, h_1, h_2; x) \mid h_0 = g^x \ \wedge \ (h_1 = h^x \ \vee \ h_2 = h^x)\}.$$

a) *Give a Σ-protocol for relation R and show that it is complete, special sound, and honest-verifier zero-knowledge.*

b) *Let $\mathcal{H}$ denote a cryptographic hash function. Turn the above Σ-protocol into a non-interactive Σ-proof (using the Fiat-Shamir heuristic) and show how the proof is verified.*

4) Let $\langle g \rangle$ be a cyclic group of order n, where n is a large prime. Further, let $h \in \langle g \rangle$ denote a random group element, such that $\log_g h$ is unknown to anyone.

We consider a secret sharing scheme with a dealer D and participants P_1, P_2, P_3. Let $s \in \mathbb{Z}_n$ be a secret to be distributed. Suppose the dealer picks shares s_1, s_2, s_3 as follows, for a random $r \in_R \mathbb{Z}_n$:

$$s_1 = r, \qquad s_2 = s - r \bmod n, \qquad s_3 = s,$$

and sends in private s_i to P_i, for $i = 1, 2, 3$.

a) *Explain which subsets of participants are qualified (i.e., are able to reconstruct the secret) and which subsets are not qualified.*

b) *Using g, extend the basic secret sharing scheme to a Feldman VSS scheme. Describe the distribution protocol and the reconstruction protocol. Explain the security properties of your scheme.*

c) *Using h in addition to g, show how to change your Feldman VSS scheme into a Pedersen VSS scheme and explain the security properties of the resulting scheme.*

1a: 2	1c: 4	2a: 4	3a: 11	4a: 3	4c: 3	homework
1b: 5	1d: 4	2b: 6	3b: 4	4b: 4		min. 0, max. 5

The final mark is the total number of points divided by 5, rounded to the nearest integer, but not exceeding 10.

Cryptographic Protocols (2WC01)
Exam, April 28, 2005, 9:00–12:00am

Solve the following problems, providing full motivation for the correctness and completeness of your solution.

Use of a simple, non-programmable pocket calculator is allowed, but not necessary. All other electronic equipment is not allowed.

Hand in your answer pages, not your scrap paper. GOOD LUCK!

Throughout, let $\langle g \rangle$ be a cyclic group of order n, where n is a large prime. Let h denote an arbitrary, fixed element of $\langle g \rangle$, $h \neq 1$.

1) Consider distributions X, Y, Z given by

$$\begin{aligned} X &= \{(e, f) \mid e \in_R \langle g \rangle, f \in_R \langle g \rangle\}, \\ Y &= \{(g^r, h^r m) \mid r \in_R \mathbb{Z}_n, m \in_R \langle g \rangle\}, \\ Z &= \{(g^r, h^r m_0) \mid r \in_R \mathbb{Z}_n\}, \qquad \text{for a fixed value } m_0 \in \langle g \rangle, \end{aligned}$$

Let Δ denote statistical distance.

a) *Show that* $\Delta(X, Y) = 0$.

b) *Show that* $\Delta(Y, Z) = 1 - 1/n$.

c) *Show that also* $\Delta(X, Z) = 1 - 1/n$, *using triangle inequalities.*

2) Consider the following computational problem. Given a pair of values $(g^r, h^r m)$ where $r \in \mathbb{Z}_n$ and $m \in \langle g \rangle$, compute m.

Show that this problem is random self-reducible.

3) Consider a homomorphic ElGamal encryption of the form $(e, f) = (g^r, h^r g^x)$, with $r \in_R \mathbb{Z}_n$. Assume that either $x = 0$ or $x = 1$. You are asked to provide a proof that indeed (e, f) is of this form without revealing any further information on r and x. That is, you are asked to provide a Σ-proof for relation R given by

$$R = \{(e, f; r, x) \mid e = g^r,\ f = h^r g^x,\ x \in \{0, 1\}\}.$$

a) *Give a Σ-protocol for relation R and show it is complete, special sound, and honest-verifier zero-knowledge. (Hint: Solve cases $x = 0$ and $x = 1$ separately, each using EQ composition, and then combine using OR-composition.)*

b) *Is the Σ-protocol witness indistinguishable?*

c) *Let $\mathcal{H}$ denote a cryptographic hash function. Turn the above Σ-protocol into a non-interactive Σ-proof (using the Fiat-Shamir heuristic) and show how the proof is verified.*

4) Recall Shamir's (t, ℓ)-threshold secret sharing scheme, $1 \leq t \leq \ell$, for sharing a secret by a dealer among participants $P_1, \ldots, P_\ell$ such that any set of t (or more) participants is able to recover the (unique) secret, but any set of $t-1$ (or less) participants is not able to find any information on the secret. Assume that the scheme is used for secrets belonging to $\mathbb{Z}_p$ for a prime p, where $p > \ell$.

Note that Shamir's scheme only protects against *passive* attacks.

a) *Show how the dealer can mount an* active *attack by deviating from the distribution protocol such that the secret recovered will not be independent of the particular set of t participants taking part in the reconstruction protocol.*

b) *Suppose that participants $P_1, \ldots, P_t$ decide to recover the secret by combining their shares. Show how participant P_t can mount an* active *attack by deviating from the reconstruction protocol such that an arbitrary given value $\widetilde{s} \in \mathbb{Z}_p$ will result as the secret recovered by $P_1, \ldots, P_t$. (Hint: participant P_t may wait until $P_1, \ldots, P_{t-1}$ have released their shares $s_1, \ldots, s_{t-1}$, before releasing its share $\widetilde{s}_t$.)*

1a: 3	1c: 4	2: 10	3a: 10	3c: 3	4a: 6
1b: 5			3b: 3		4b: 6

The final mark is the total number of points divided by 5, rounded to the nearest integer.

Cryptographic Protocols (2WC01)
Exam, March 14, 2005, 2:00–5:00pm

Solve the following problems, providing full motivation for the correctness and completeness of your solution.

Use of a simple, non-programmable pocket calculator is allowed, but not necessary. All other electronic equipment is not allowed.

Hand in your answer pages, not your scrap paper. GOOD LUCK!

---

1) Consider distributions U and V given by

$$\begin{aligned} U &= \{u \mid u \in_R \mathbb{Z}_m\}, \text{ and} \\ V &= \{u + k \mid u \in_R \mathbb{Z}_m\}, \end{aligned}$$

for positive integers m and k (with $\mathbb{Z}_m = \{0, \ldots, m-1\}$).

Let Δ denote statistical distance.

a) *Assume $k \leq m$. Compute $\Delta(U, V)$.*

b) *What is $\Delta(U, V)$ if $k > m$?*

2) Let $\langle g \rangle$ be a cyclic group of order n, where n is a large prime. Consider the following two protocols between parties A and B connected by an insecure communication channel: Protocol I for sending a message $m \in \langle g \rangle$, $m \neq 1$, securely from party A to party B, and Protocol II for sending a message $b \in \{0, 1\}$, securely from party A to party B (with $\oplus$ denoting exclusive-or).

Protocol I

Party A		Party B
$x_A \in_R \mathbb{Z}_n^*$		
$y_A \leftarrow m^{x_A}$	$\xrightarrow{y_A}$	
		$x_B \in_R \mathbb{Z}_n^*$
	$\xleftarrow{y_{AB}}$	$y_{AB} \leftarrow y_A^{x_B}$
$y_B \leftarrow y_{AB}^{1/x_A}$		
	$\xrightarrow{y_B}$	
		$m' \leftarrow y_B^{1/x_B}$

Protocol II

Party A		Party B
$b_A \in_R \{0, 1\}$		
$c_A \leftarrow b \oplus b_A$	$\xrightarrow{c_A}$	
		$b_B \in_R \{0, 1\}$
	$\xleftarrow{c_{AB}}$	$c_{AB} \leftarrow c_A \oplus b_B$
$c_B \leftarrow c_{AB} \oplus b_A$		
	$\xrightarrow{c_B}$	
		$b' \leftarrow c_B \oplus b_B$

The object of both protocols is that the message sent remains completely hidden for other parties than A and B, and that the message cannot be modified by other parties than A or B.

a) *Verify that $m' = m$ and $b' = b$ if A and B follow protocols I and II, respectively.*

Next, answer the following questions with 'yes' or 'no'; in case of a 'yes' describe the relevant computational assumption (if any), in case of a 'no' show an attack.

b) *Is protocol I secure against* **passive** *attacks?*

c) *Is protocol I secure against* **active** *attacks?*

d) *Is protocol II secure against* **passive** *attacks?*

e) *Is protocol II secure against* **active** *attacks?*

3) Let $\langle g \rangle$ be a cyclic group of order n, where n is a large prime. Consider an (ℓ, ℓ)-threshold ElGamal cryptosystem for parties $P_1, \ldots, P_\ell$ with public key h given by $h = g^x$ and $x = \sum_{i=1}^{\ell} x_i$, where x_i denotes party P_i's private share, $1 \leq i \leq \ell$, and let $h_i = g^{x_i}$ denote party P_i's (public) verification key.

Recall that given an encryption $(a, b) = (g^r, h^r m)$, $r \in_R \mathbb{Z}_n$, of a message $m \in \langle g \rangle$, the threshold decryption protocol requires each party P_i to release value $d_i = a^{x_i}$ and a Σ-proof that $\log_a d_i = \log_g h_i$.

Now, consider the following modification of the threshold decryption protocol. Let $H \in \langle g \rangle$ denote a public key of an additional party Q, and let $X = \log_g H$ denote party Q's private key. Instead of releasing $d_i = a^{x_i}$ in the clear, each party P_i *encrypts* the value d_i under Q's public key and provides a Σ-proof that the encryption is done correctly. That is, each party P_i releases an encryption $(e_i, f_i) = (g^{s_i}, H^{s_i} d_i)$, $s_i \in_R \mathbb{Z}_n$, and a Σ-proof for the relation:

$$R_i = \{(a, H, e_i, f_i, h_i; s_i, x_i) \mid e_i = g^{s_i}, f_i = H^{s_i} a^{x_i}, h_i = g^{x_i}\}.$$

a) *Show how party Q is able to recover message m using its private key X, given (a, b) and correct encryptions $(e_1, f_1), \ldots, (e_\ell, f_\ell)$.*

b) *Show how to construct an encryption (e, f) of message m for public key H, given (a, b) and correct encryptions $(e_1, f_1), \ldots, (e_\ell, f_\ell)$, but* without *using private key X.*

c) *Give a Σ-protocol for relation R_i and show it is complete, special sound, and honest-verifier zero-knowledge. (Hint: Use Schnorr's protocol both for e_i and h_i, Okamoto's protocol for f_i, and combine these three protocols using EQ-composition.)*

d) *Let $\mathcal{H}$ denote a cryptographic hash function. Turn the above Σ-protocol into a non-interactive Σ-proof (using the Fiat-Shamir heuristic) and show how the proof is verified.*

4) See the previous problem. Describe how the scheme can be extended for (t, ℓ)-threshold ElGamal cryptosystems, $1 \leq t \leq \ell$, by describing the necessary changes: let the shares x_i be defined as in Shamir's threshold scheme, and explain how parties $P_1, \ldots, P_\ell$ and party Q proceed to perform their decryption steps.

1a:	7	2a:	2	2c:	3	2e:	3	3a:	3	3c:	10	4:	7
1b:	3	2b:	3	2d:	3			3b:	4	3d:	2		

The final mark is the total number of points divided by 5, rounded to the nearest integer.

Cryptographic Protocols (2WC01)
Exam, May 12, 2004, 9:00–12:00am

Solve the following problems, providing full motivation for the correctness and completeness of your solution.

Use of a simple, non-programmable pocket calculator is allowed, but not necessary. All other electronic equipment is not allowed.

Hand in your answer pages, not your scrap paper. GOOD LUCK!

The topic of the **four** problems below is the construction of a particular electronic voting scheme. Throughout, let $\langle g \rangle$ be a cyclic group of order n, where n is a large prime. Further, let $h \in \langle g \rangle$ denote a random group element, such that $\log_g h$ is unknown to anyone.

1) Each voter casts either a 'yes'-vote or a 'no'-vote, represented by $1 \in \mathbb{Z}_n$ and $-1 \in \mathbb{Z}_n$, respectively. As a first step, a voter commits to its vote $v \in \{1, -1\}$ by choosing a value $r \in_R \mathbb{Z}_n$ and broadcasting the commitment $C = g^v h^r$.

Consider distributions X, Y, Z given by

$$\begin{aligned} X &= \{gh^r \mid r \in_R \mathbb{Z}_n\}, \\ Y &= \{h^r \mid r \in_R \mathbb{Z}_n\}, \\ Z &= \{g^{-1}h^r \mid r \in_R \mathbb{Z}_n\}. \end{aligned}$$

Let Δ denote statistical distance.

a) *Compute $\Delta(X, Y)$, $\Delta(X, Z)$, and $\Delta(Y, Z)$.*

b) *Does C reveal any information about the value of v?*

2) To prevent a voter from casting an illegal vote $v \notin \{1, -1\}$, the voter is required to prove that $v \in \{1, -1\}$ holds, without disclosing any further information on v.

a) *Using OR-composition, give a Σ-protocol for the relation*

$$R = \{(C; v, r) \mid C = g^v h^r, v \in \{1, -1\}\}.$$

Hence C is public and v, r is the witness, which is known only to the voter. Prove that the Σ-protocol is complete, special sound, and honest-verifier zero-knowledge.

b) *Let $\mathcal{H}$ denote a cryptographic hash function. Turn the above Σ-protocol into a non-interactive Σ-proof (using the Fiat-Shamir heuristic) and show how the proof is verified.*

See overleaf.

3) The votes will be counted by ℓ talliers $T_1, \ldots, T_\ell$. Each voter splits its vote v and commitment C into ℓ parts $C_1, \ldots, C_\ell$ such that $C = \prod_{j=1}^{\ell} C_j$. To do so, a voter chooses $v_1, r_1, \ldots, v_\ell, r_\ell \in_R \mathbb{Z}_n$ subject to the condition that $\sum_{j=1}^{\ell} v_j = v$ and $\sum_{j=1}^{\ell} r_j = r$ and sets $C_j = g^{v_j} h^{r_j}$ for $j = 1, \ldots, \ell$.

A voter broadcasts the values $C_1, \ldots, C_\ell$. In addition, a voter sends the values v_j, r_j in private to tallier T_j, for $j = 1, \ldots, \ell$.

a) *Show that indeed* $C = \prod_{j=1}^{\ell} C_j$.

b) *Show that even if* $\ell - 1$ *talliers collude and combine all their shares* v_j, r_j*, the value of* v *remains completely hidden. Without loss of generality, you may assume that tallier* T_1 *is honest, whereas talliers* $T_2, \ldots, T_\ell$ *try to cheat.*

4) Finally, assume that ℓ' voters $V_1, \ldots, V_{\ell'}$ take part in the election. Voter V_i proceeds as above producing values for a vote $v_i \in \{1, -1\}$ indexed by i, $1 \leq i \leq \ell'$: commitment C_i accompanied by a non-interactive proof that $v_i \in \{1, -1\}$ and values $C_{1,i}, \ldots, C_{\ell,i}$. The corresponding values $v_{j,i}, r_{j,i}$ are sent in private to the talliers T_j, for $j = 1, \ldots, \ell$, respectively.

a) *Recall the homomorphic property for Pedersen's commitment scheme. Show how tallier* T_j *computes values* $V_j, R_j \in \mathbb{Z}_n$ *such that* $\prod_{i=1}^{\ell'} C_{j,i} = g^{V_j} h^{R_j}$*, for* $j = 1, \ldots, \ell$*, and show how the correctness of these values is verified.*

b) *Show how the election result* $V = \sum_{i=1}^{\ell'} v_i$ *is computed from the values* $V_1, R_1, \ldots, V_\ell, R_\ell$.

c) *Consider the case that a single tallier tries to cheat. Is the integrity of the election result protected information-theoretically: that is, is a computationally unbounded tallier able to see to it that an election result* $V' \neq V$ *results, which still passes verification? Explain your answer.*

1a: 7	2a: 10	3a: 2	4a: 8
1b: 3	2b: 4	3b: 10	4b: 3
			4c: 3

The final mark is the total number of points divided by 5, rounded to the nearest integer.

Cryptographic Protocols (2WC01)
Exam, March 15, 2004, 9:00–12:00am

Solve the following problems, providing full motivation for the correctness and completeness of your solution.

Use of a simple, non-programmable pocket calculator is allowed, but not necessary. All other electronic equipment is not allowed.

Hand in your answer pages, not your scrap paper. GOOD LUCK!

The topic of the **four** problems below is the construction of a particular verifiable secret sharing scheme. Throughout, let $\langle g \rangle$ be a cyclic group of order n, where n is a large prime. Note that $\mathbb{Z}_n^* = \mathbb{Z}_n \setminus \{0\}$.

1) Recall that the Diffie-Hellman (DH) problem is as follows: given g^x, g^y, compute g^{xy}, where $x, y \in \mathbb{Z}_n$. Consider the following variant of the Diffie-Hellman problem: given g^x, g^y, compute $g^{x/y}$, where $x, y \in \mathbb{Z}_n^*$. We call this the DH-INV problem.

Show that the DH-INV problem is random self-reducible by showing how to transform an input pair g^x, g^y into a pair $g^{x'}, g^{y'}$ for suitably chosen, uniformly distributed values $x', y' \in \mathbb{Z}_n^*$, and showing how to extract the value of $g^{x/y}$ from the value of $g^{x'/y'}$.

2) Consider distributions X, Y, Z given by

$$\begin{aligned} X &= \{(g^x, g^y) \mid x \in_R \mathbb{Z}_n, y \in_R \mathbb{Z}_n\}, \\ Y &= \{(g^x, g^y) \mid x \in_R \mathbb{Z}_n, y \in_R \mathbb{Z}_n^*\}, \\ Z &= \{(g^x, g^y) \mid x \in_R \mathbb{Z}_n^*, y \in_R \mathbb{Z}_n^*\}. \end{aligned}$$

Let Δ denote statistical distance.

a) *Show that $\Delta(X, Y) = 1/n$.*

b) *Show that also $\Delta(Y, Z) = 1/n$.*

c) *Show that $\Delta(X, Z) \leq 2/n$, by the triangle inequality for Δ.*

It follows that the statistical distances $\Delta(X, Y), \Delta(Y, Z), \Delta(X, Z)$ are negligible if we take $n \approx 2^k$ for a security parameter k.

As a conclusion from (1) and (2) we have that the problem of computing $g^{x/y}$ from g^x, g^y is hard, where $x, y \in \mathbb{Z}_n$ and the special cases $x = 0$ or $y = 0$ do not really matter.

See overleaf.

3) We consider a secret sharing scheme with a dealer D and participants $P_1, \ldots, P_\ell$, $\ell \geq 1$. Each participant P_i has a private key $x_i \in Z_n^*$ and a public key $h_i = g^{x_i}$, $1 \leq i \leq \ell$. The secrets to be distributed by D and to be reconstructed by $P_1, \ldots, P_\ell$ are random elements of $\langle g \rangle$.

- **Distribution protocol.** The dealer chooses $z \in_R \mathbb{Z}_n$, and sets the secret s to $s = g^z$. The dealer chooses $z_2, \ldots, z_\ell \in_R \mathbb{Z}_n$ and sets $z_1 = z - \sum_{i=2}^{\ell} z_i \pmod{n}$. Then the dealer broadcasts the values $e_i = h_i^{z_i}$, using the public keys h_i of the participants, for $i = 1, \ldots, \ell$.
- **Reconstruction protocol.** Each participant P_i sets $s_i = e_i^{1/x_i}$, using its private key x_i. The secret s is reconstructed as $s = \prod_{i=1}^{\ell} s_i$.

Assume that the dealer and the participants follow the protocol.

a) *Show that reconstruction works, hence that $s = g^z$ holds.*

b) *Fix a participant P_i. Show that a passive attacker who just sees the values h_i and e_i cannot compute g^{z_i}, assuming that the above DH-INV problem is hard.*

c) *Is the secret s protected information-theoretically?*

4) Next, we turn the above scheme into a verifiable secret sharing scheme by extending the reconstruction protocol as follows.

- **Extended reconstruction protocol.** Each participant P_i sets $s_i = e_i^{1/x_i}$, using its private key x_i, and provides a proof showing that the value of s_i is correct with respect to h_i and e_i. The secret s is reconstructed as $s = \prod_{i=1}^{\ell} s_i$.

a) *Using EQ-composition, give a Σ-protocol for the relation*

$$R_i = \{(h_i, e_i, s_i; x_i) \mid h_i = g^{x_i}, e_i = s_i^{x_i}\}.$$

Hence h_i, e_i, s_i are public and x_i is the witness, which is known only to P_i. Prove that the Σ-protocol is complete, special sound, and honest-verifier zero-knowledge.

b) *Let $\mathcal{H}$ denote a cryptographic hash function. Turn the above Σ-protocol into a non-interactive Σ-proof (using the Fiat-Shamir heuristic) and show how the proof is verified.*

c) *Explain why the dealer cannot give out inconsistent shares to the participants.*

1:	10	2a:	4	3a:	4	4a:	10
		2b:	3	3b:	7	4b:	3
		2c:	3	3c:	3	4c:	3

The final mark is the total number of points divided by 5, rounded to the nearest integer.