"Cheat sheet" Exams 2WC09/2WC12, Fall 2012

At the exams, use of a simple, non-programmable pocket calculator is allowed. All other electronic equipment is not allowed, nor any notes or books.

The following formulas will be provided at the exams.

Shannon entropy of r.v. X taking values in $\{x_1, \ldots, x_n\}$ with probability $p_i = \Pr[X = x_i]$:

$$H(X) = -\sum_{i=1}^{n} p_i \log_2 p_i$$

Digital Signature Algorithm (DSA), for hash function h.

Key generation. Given primes p, q such that $p|(q-1)$ and an element g of order p in $\mathbb{Z}_q^*$, choose private key m_U uniform at random in $\mathbb{Z}_p^*$, and set public key $c_U = g^{m_U} \bmod q$.

Signature generation. Given message M, choose r uniform at random in $\mathbb{Z}_p^*$, and set

$$R = (g^r \bmod q) \bmod p, \qquad S = (h(M) + m_U R) r^{-1} \bmod p$$

Signature verification. Given message M, signature (R, S), check if

$$R = (g^x c_U^y \bmod q) \bmod p, \quad \text{where } x = h(M)S^{-1} \bmod p,\ y = RS^{-1} \bmod p$$

Addition formulas for elliptic curve E over any finite field of characteristic p.

Let $P_3 = P_1 + P_2$.

If $P_1 = \mathcal{O}$, then $P_3 = P_2$.
If $P_2 = \mathcal{O}$, then $P_3 = P_1$.
If $P_1 = -P_2$, then $P_3 = \mathcal{O}$.
Otherwise, let $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$, then $P_3 = (x_3, y_3)$ is given as follows.

Case $p = 2$	Case $p \neq 2$
$E : y^2 + xy = x^3 + ax^2 + c$	$E : y^2 = x^3 + ax^2 + bx + c$
$x_3 = x_1^2 + \frac{c}{x_1^2}$	$x_3 = \lambda^2 - a - x_1 - x_2$
$y_3 = x_1^2 + (x_1 + \frac{y_1}{x_1})x_3$	$y_3 = \lambda(x_1 - x_3) - y_1$

$$\lambda = \begin{cases} \frac{3x_1^2 + 2ax_1 + b}{2y_1}, & x_1 = x_2 \\ \frac{y_2 - y_1}{x_2 - x_1}, & x_1 \neq x_2 \end{cases}$$