Exercises 2WC12 week 6

Exercise 1

The elements of the finite field $\mathbb{F}_{32}$ are $a_0 + a_1\alpha + \ldots + a_4\alpha^4$, with $a_0, a_1, \ldots a_4 \in \{0, 1\}$. Here α satisfies $\alpha^5 + \alpha^3 + 1 = 0$.

Alice and Bob choose $g = 1 + \alpha^3$ as generator of the multiplicative group $\mathbb{F}_{32}^*$. Alice chooses 2 as private key, and Bob chooses 3 as private key.

Show in detail the computations that both have to do to run the Diffie-Hellman protocol.

Exercise 2

DSA works as follows:

System parameters:
- a prime $p \equiv 1 \pmod{q}$, where q is a prime of 160 bits and p is 1024 bits,
- a generator g of order q in $\mathbb{F}_p^*$,

Key pair:
- a random $x \in \mathbb{Z}_{q-1}$ as private key,
- $y = g^x$ as public key,

Signature generation:
- compute the hash h of the to be signed message,
- take a random $k \in \mathbb{Z}_{q-1}$,
- compute $r \equiv (g^k \pmod{p}) \pmod{q}$,
- compute $s = (h + xr)/k \pmod{q}$,
- the signature is (r, s),

Signature verification:
- compute the hash h of the signed message,
- compute $a = hs^{-1} \pmod{q} and b = rs^{-1} \pmod{q}$,
- compute $v = (g^a y^b \pmod{p}) \pmod{q}$,
- accept if and only if $v = r$.

Show that using the same k in generating signatures on two different messages leaks the private key. Hint: look at the difference of the two signatures.