Exercises 2WC12 week 5

Exercise 1

A smartcard using RSA for digital signatures contains a CRT-private key, consisting of $p, q, d_p \equiv d \pmod{p-1}, d_q \equiv d \pmod{q-1}, u \equiv p^{-1} \pmod{q}$. The corresponding public key consists of $n = 855233$, $e = 65537$.

Somebody grills the smartcard in a microwave, and then asks it to sign the message $m = 123456$. The smartcard returns the value $s = 291643$.

Using this, find the complete private key p, q, d_p, d_q, u.

Exercise 2

For the prime $p = 1013$, the generator $g = 3$ generates the full group $\mathbb{Z}_p^*$.

ElGamal in $\mathbb{Z}_p^*$ with key pair $x, y = g^x$ encrypts a message m as follows:

- generate a random $k \in \mathbb{Z}_{p-1}$ and compute $c_1 = g^k$,
- compute $c_2 = my^k$,
- the ciphertext is (c_1, c_2).

and decryption is $m = c_2/c_1^x$.

a) Encrypt using ElGamal the message $m = 42$ with the public key $y = 224$ and the random number $k = 654$.

b) Decrypt using ElGamal the ciphertext $(c_1, c_2) = (954, 907)$ with the private key $x = 899$.

c) Explain how an attacker who intercepts an ElGamal ciphertext and somehow knows k, is able to decrypt, without knowledge of the private key x.