9

Names: Erwin van Duijnhoven and Rick Staals
Student IDs: 0719562 and 0716184

Exercise 1

$3 \in \mathbb{F}_{1013}^*$ *generates a group of order* 1012*, so it generates the whole multiplicative group of the finite field.*
Alice's public key is $h_A = 224$*. Use ElGamal encryption to encrypt the message* $m = 42$ *to her using the "random" value* $k = 654$*.*
We send $(g^k, m \cdot h_A^k)$.

$\frac{1}{2}/1$

show computations!

$$g^k = 3^{654} \equiv 628 \mod 1013$$
$$h_A^k = 224^{654} \equiv 1004 \mod 1013$$
$$m \cdot h_A^k = 42 \cdot 1004 \equiv 635 \mod 1013$$

Therefore we send $(628, 635)$.

Exercise 2

Compute the product of all monic, irreducible polynomials of degree 6 *over* $\mathbb{F}_2$*.*
The monic, irreducible polynomials of degree 6 over $\mathbb{F}_2$ are

- $x^6 + x + 1$
- $x^6 + x^3 + 1$
- $x^6 + x^4 + x^2 + x + 1$
- $x^6 + x^4 + x^3 + x + 1$
- $x^6 + x^5 + 1$
- $x^6 + x^5 + x^2 + x + 1$
- $x^6 + x^5 + x^3 + x^2 + 1$
- $x^6 + x^5 + x^4 + x + 1$
- $x^6 + x^5 + x^4 + x^2 + 1$

2/2

The product of these polynomials is

$$x^{54} + x^{53} + x^{51} + x^{50} + x^{48} + x^{46} + x^{45} + x^{43} + x^{42} + x^{33} + x^{32} + x^{30}$$
$$+ x^{29} + x^{27} + x^{25} + x^{24} + x^{22} + x^{21} + x^{12} + x^{11} + x^9 + x^8 + x^6 + x^4 + x^3 + x + 1$$

Exercise 3

$3 \in \mathbb{F}_{1013}^*$ *generates a group of order* 1012, *so it generates the whole multiplicative group of the finite field. Solve the discrete logarithm problem* $g = 3, h = 224$ *using the Baby-step Giant-step algorithm.*

$m = \lfloor \sqrt{1012} \rfloor = 31$. Now $k = k_0 + k_1 m$. First we produce the list of $(i, 3^i)$ for $i \in \{0, \dots 31\}$. For esthetical reasons, this list is not included. $3^{32} \equiv 257 \mod 1013$ and $3^{-32} \equiv 473 \mod 1013$.

Now we calculate the list $224 \cdot 473^j \mod 1013$ until we find a value in right hand side of the list of $(i, 3^i)$. We find the combination $j = 19, i = 4$, so $k = 19 \cdot 32 + 4 = 612$

$2\frac{1}{2}/3$

do include the lists!

1/1

Exercise 4

$3 \in \mathbb{F}_{1013}^*$ generates a group of order $1012 = 4 \cdot 11 \cdot 23$. Solve the discrete logarithm problem $g = 3, h = 321$ by using the Pohlig-Hellman attack, i.e. find an integer $0 < k < 1012$ such that $h = g^k$ by computing first k modulo $2, 4, 11,$ and 23 and then computing k using the Chinese Remainder Theorem.

We first calculate k_2, k_{11} and k_{23}:

$$\begin{aligned} k &\equiv k_2 \mod 2^2 \\ k &\equiv k_{11} \mod 11^1 \\ k &\equiv k_{23} \mod 23^1. \end{aligned}$$

$k_2 = c_0 + c_1 \cdot 2$ with $c_0, c_1 \in \{0, 1\}$.

- $321^{506} \equiv 1 \equiv 3^{c_0 \cdot 506} \mod 1013 \Rightarrow c_0 = 0$
- $321 \cdot 3^{-c_0} = 321$
  $321^{253} \equiv -1 \equiv 3^{c_1 \cdot 506} \mod 1013 \Rightarrow c_1 = 1.$

Therefore $k_2 = 0 + 1 \cdot 2 = 2$
$k_{11} \in \{0, \ldots, 10\}$.

- $321^{92} \equiv 804 \equiv 3^{k_{11} \cdot 92} \mod 1013 \Rightarrow k_{11} = 6.$

$k_{23} \in \{0, \ldots, 22\}$.

- $321^{44} \equiv 190 \equiv 3^{k_{23} \cdot 44} \mod 1013 \Rightarrow k_{23} = 13.$

Now we use the Chinese Remainder Theorem to find k:

$$\begin{aligned} M_2 = 253, y_2 &\equiv M_2^{-1} \equiv 1 \mod 4 \\ M_{11} = 92, y_{11} &\equiv M_{11}^{-1} \equiv 3 \mod 11 \\ M_{23} = 44, y_{23} &\equiv M_{23}^{-1} \equiv 11 \mod 23 \\ \Rightarrow k \equiv 2 \cdot 253 \cdot 1 + 6 \cdot 92 \cdot 3 + 13 \cdot 44 \cdot 11 &\equiv 358 \mod 1012 \end{aligned}$$

This means $k \equiv 358 \mod 1013$.

Exercise 5

The ElGamal signature scheme works as follows: The system parameters are a finite field $\mathbb{F}_p$, an element $g \in E(\mathbb{F}_p)$, and the order l of g. Furthermore a hash function H is given along with a way to interpret $H(m)$ as an element of $\mathbb{F}_q$.
Alice creates a public key by selecting an integer $1 < a < l$ and computing $h_A = g^a$; a is Alice's long-term secret and h_A is her public key.
To sign a message m, Alice first computes $H(m)$, then picks a random integer $1 < k < l$ and computes $R = g^k$. She then interprets R as an integer and reduces it modulo l; call this result r; if $r = 0$ she starts over. Then she calculates

$$s = k^{-1}(H(m) + r \cdot a) \mod l.$$

If $s = 0$ she starts over with a different choice of k.
The signature is the pair (r, s).
To verify a signature (r, s) on a message m by user Alice with public key h_A, Bob first computes $H(m)$, then computes $w \equiv s^{-1} \mod l$, then computes $u_1 \equiv H(m) \cdot w \mod l$ and $u_2 \equiv r \cdot w \mod l$ and finally computes

$$R' = g^{u_1} \cdot h_A^{u_2}.$$

Bob accepts the signature as valid if $R' \equiv r \mod l$.

5a

Show that a signature generated by Alice will pass as a valid signature by showing that $R = R'$.

1/1

$$\begin{aligned} R' &\equiv g^{u_1} \cdot h_A^{u_2} \\ &\equiv g^{H(m)\cdot w} \cdot g^{a \cdot r \cdot w} \\ &\equiv g^{(H(m)+a\cdot r)w} \\ &\equiv g^{s\cdot k \cdot w} \\ &\equiv g^k \\ &\equiv R \mod l \end{aligned}$$

5b

Show how to obtain Alice's long-term secret a when given the random value k for one signature (r, s) on some message m.

1/1

$$\begin{aligned} s &\equiv k^{-1}(H(m) + r \cdot a) \mod l \\ \Rightarrow s \cdot k &\equiv H(m) + r \cdot a \mod l \\ \Rightarrow s \cdot k - H(m) &\equiv r \cdot a \mod l \\ \Rightarrow a &\equiv r^{-1}(s \cdot k - H(m)) \mod l \end{aligned}$$

5c

You find two signatures made by Alice. You know that she is using the ElGamal signature scheme over $\mathbb{F}_{2027}$ *and that the order of the generator is* $l = 1013$*. The signatures are for* $H(m_1) = 345$ *and* $H(m_2) = 567$ *and are given by* $(r_1, s_1) = (365, 448)$ *and* $(r_2, s_2) = (365, 969)$*. Compute (a candidate for) Alice's long-term secret* a *based on these signatures, i.e. break the system.*

First we calculate k

$$\begin{cases} 448 \equiv k^{-1}(345 + 365a) \mod 1013 \\ 969 \equiv k^{-1}(567 + 365a) \mod 1013 \end{cases}$$

$$\begin{aligned} \Rightarrow 448k - 345 &\equiv 969k - 567 \mod 1013 \\ \Rightarrow 521k &\equiv 222 \mod 1013 \\ \Rightarrow k &\equiv 222 \cdot 521^{-1} \mod 1013 \\ \Rightarrow k &\equiv 222 \cdot 35 \mod 1013 \\ \Rightarrow k &\equiv 679 \mod 1013 \end{aligned}$$

Now that we know k, we use the result of 5b to calculate a.

$$\begin{aligned} a &\equiv r^{-1}(s \cdot k - H(m)) \mod l \\ &\equiv 365^{-1}(679 \cdot 448 - 345) \mod 1013 \\ &\equiv 974 \mod 1013 \end{aligned}$$

1/1