Cryptography

Prof. Dr. Klaus Meer, Ameen Naif

Exercise Sheet 6
Version 05.07.2019

Exercise 1.

Factorize 299 using **Pollard's** $(p-1)$**-algorithm** with $B = 5$.

Exercise 2.

Let $p \in \mathbb{N}$ be a prime, $g \in \mathbb{Z}_p^*$ a generator of $(\mathbb{Z}_p^*, \cdot)$.

(a) **Base change**: If $h \in \mathbb{Z}_p^*$ is another generator of $(\mathbb{Z}_p^*, \cdot)$, then it holds: $\forall a \in \mathbb{Z}_p^*$: $log_g(a) = log_h(a) \cdot log_g(h)$.

(b) Use **Shank's algorithm** to find $x = log_5(20)$ in $\mathbb{Z}_{47}^*$.

Exercise 3.

Let Bob's public **ElGamal key** be $(p, g, \beta) = (101, 2, 11)$.

(a) Find Bob's private ElGamal key b.

(b) Find the plaintext m of the ciphertext $(a_1, a_2) = (64, 79)$ sent to Bob from Alice.

Exercise 4.

Let $p(x) = x^3 + x + 1$ and $q(x) = x^2 + 1 \in \mathbb{Z}_2[x]$.

(a) Compute $p(x) \cdot q(x)$ and $q(x)$ mod $p(x)$.

(b) Compute $x^5 + x^4 + x^2 + x + 1$ mod $p(x)$.

(c) Find an **irreducible** polynomial in $\mathbb{Z}_2[x]$ of degree 3.

(d) Find all elements of the ring $(\mathbb{Z}_2[x]/p, +, \cdot)$. Is the ring $(\mathbb{Z}_2[x]/p, +, \cdot)$ a field?

Exercise 5.

Let $\mathbb{F}$ be a field and $f(x) = x^3 + ax + b$ be a fixed polynomial in $\mathbb{F}[x]$.

(a) Show that $(x - x_0)$ is a factor of f if $f(x_0) = 0$, where $x_0 \in \mathbb{F}$ is fixed.

(b) Show that: $4a^3 + 27b^2 = 0 \iff f$ has a root of multiplicity at least 2.

Exercise 6.

Let $\mathbb{F} := \mathbb{Z}_{11}$ and consider the elliptic curve $\widetilde{E}$ defined by $y^2 = x^3 + x + 6$ over $\mathbb{F}$.

(a) Find all points on the elliptic curve $\widetilde{E}$.

(b) Let $Q_1 = (8, 3)$ and $Q_2 = (3, 6)$ be points on the elliptic curve $\widetilde{E}$, compute $Q_1 \oplus Q_2$ and $5Q_1$.

(c) Let $P = (2, 4)$ be a generator of the group $(\widetilde{E}, \oplus)$ and suppose that the private key is $n_B = 3$.

i) Compute the public key $Q = n_B \cdot P$.

ii) Encrypt the plaintext $M := (7, 2) \in \widetilde{E}$ using as random value $n_A = 4$ and then decrypt the obtained ciphertext $(A_1, A_2) \in \widetilde{E}^2$.

Exercise 7.

How can you construct a finite field of $n \in \mathbb{N}$ elements, if one exists? Is there are one of 9 elements? Construct it, if one exists.