Review Exercise Advanced Methods of Cryptography

Prof. Dr. Rudolf Mathar, Michael Reyer, Henning Maier

07.08.2013, WSH 24 A 407, 10:00h

Exercise 1. An archaeologist found a secret entrance to an ancient English[1] pyramid. The inscription of the massive door reveals:

A	I	V	Z	Z	Q	U	V	K	V	Q	Q	V	I
0	8	21	25	25	16	20	21	10	21	16	16	21	8

Z	W	F	S	E	H	Q	J	J	A	V	S	B	V
25	22	5	18	4	7	16	9	9	0	21	18	1	21

The archaeologist already found out that the ciphertext space is $\mathcal{C} = \{A, B, \ldots, Z\}$ and that an affine cipher is used.

(a) What is the cardinality of the message space $\mathcal{M}$ and of the key space $\mathcal{K}$?

(b) Calculate the estimator of the index of coincidence I_c and decide if this is a monoalphabetic or a polyalphabetic cipher.

(c) Help the archaeologist to decipher the inscription: Give the encryption and decryption rule and decipher the first eight letters of the cryptogram to verify your results. What is the key?

Hint: The most frequent letters in English are:

letter	E	T	A	O	I	N
frequency	12.2	9.10	8.12	7.68	7.31	6.95

Exercise 2. Let φ be the Euler function. Moreover, let $p \neq q$ be prime numbers and $n = p\,q$.

(a) Show that $\varphi(p\,q) = \varphi(p)\,\varphi(q)$ holds.

(b) Show that n may be efficiently factorized if $\varphi(n)$ is known.

(c) Factorize $n = 367080319$ by means of $\varphi(n) = 367042000$.

Another variant for factorization of a natural number m was developped by Pierre de Fermat. He has utilized

$$m = x^2 - y^2 = (x - y)\,(x + y) \quad x, y \in \mathbb{N}_0 \tag{1}$$

for factorization.

(d) Factorize $n = 367080319$ utilizing (1).

(e) Is it possible to find $x, y \in \mathbb{N}_0$ for all natural numbers $m > 2$ such that (1) is fulfilled? Give a reason.

Exercise 3. Alice wants to use the triple $(p, a, y) = (137, 3, 97)$ as public ElGamal key.

(a) Show that this is a valid ElGamal key.

(b) Determine the plaintext of Alice's message $(c_1, c_2) = (81, 7)$ without calculating the private key x.

Alice utilizes this key for signing the messages $h(m_1) = 106$ and $h(m_2) = 99$ with the signatures $(r_1, s_1) = (13, 63)$ and $(r_2, s_2) = (13, 62)$.

(c) What did Alice do wrong?

(d) Calculate her private key x.

Exercise 4. Consider the following function:

$$E : Y^2 = X^3 + 2X + 6.$$

(a) Does E describe an elliptic curve in the field $\mathbb{F}_7$? Give a reason.

(b) Determine all points and their inverses in the group.

(c) What is the order of the group?

It is difficult to obtain the discrete logarithm a of Q to the base P for two points P, Q of an elliptic curve E. A possible approach is the application of the Pollard ρ-factoring method. The idea behind this method is to find numbers $c, d, c', d' \in \mathbb{Z}$ for two given points P, Q on the elliptic curve with $\gcd(d - d', \mathrm{ord}(P)) = 1$ such that the following equation holds:

$$cP + dQ = c'P + d'Q. \tag{2}$$

(d) Compute the discrete logarithm a of Q to base P by means of (2).

An oracle provides us the values $c = 2$, $d = 4$, $c' = -1$, $d' = -3$, $P = (4, 1)$, $Q = (1, 3)$, $4Q = (3, 5)$, and $-3Q = (5, 6)$. Assume that P is a generator.

(e) Show that equation (2) is fulfilled for these values and compute the discrete logarithm a of Q to base P.