Review Exercise Advanced Methods of Cryptography

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

05.03.2014

Exercise 1. Consider the following cryptosystem with message space $\mathcal{M}$ and ciphertext space $\mathcal{C}$
as $\mathcal{M} = \mathcal{C} = \{0, 1, 2\}^2$. A message $\mathbf{m} = (m_1, m_2)$ is encrypted by means of an invertible matrix $\mathbf{A} \in \mathbb{F}_3^{2\times 2}$ as follows.

$$e(m_1, m_2) = (c_1, c_2)^T = \mathbf{A}(m_1, m_2)^T$$

This encryption scheme is used for a block cipher on messages of arbitrary length with the matrix

$$\mathbf{A} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}.$$

(a) Encrypt the message $\mathbf{m} = (1, 2, \ 1, 1)$ in the Cipher Blockchaining Mode (CBC) with initial value $C_0 = (2, 1)$.

(b) Specify the encryption and decryption rules for the Output Feedback Mode (OFB). Why is $Z_0 = C_0 = (0, 0)$ an inappropriate initial value?

In the following, the cryptosystem shall be investigated for invertible matrices of the form

$$\mathbf{A} = \begin{pmatrix} 1 & x \\ y & z \end{pmatrix} \in \mathbb{F}_3^{2\times 2}.$$

(c) Characterize the key space $\mathcal{K}$ and determine its cardinality.

(d) Specify the decryption rule $d(c_1, c_2)$.

(e) Has the system perfect secrecy, if the keys are uniformly distributed over $\mathcal{K}$, the messages are uniformly distributed over $\mathcal{M}$, and both are stochastically independent? Substantiate your answer.

Exercise 2. A public key cryptosystem for a plaintext $m = \sum_{i=1}^{n} m_i 2^{i-1}$ with $n \in \mathbb{N}$ and $m_i \in \{0, 1\}$ is given as follows:

Key Generation:

(1) Choose a random sequence $\boldsymbol{w} = (w_1, w_2, \ldots, w_n)$, with $w_i \in \mathbb{N}$, such that $w_{k+1} > \sum_{i=1}^{k} w_k$ holds for $k = 1, \ldots, n-1$.

(2) Choose $q \in \mathbb{N}$, such that $q > \sum_{i=1}^{n} w_i$ holds.

(3) Choose $r \in \mathbb{N}$ with $1 \le r < q$, such that $\gcd(r, q) = 1$ holds.

(4) Compute $\boldsymbol{\beta} = (\beta_1, \beta_2, \ldots, \beta_n)$ with $\beta_i = r w_i \mod q$.

(5) The public key is $\boldsymbol{\beta}$ and the secret key is $(\boldsymbol{w}, q, r)$.

Encryption Procedure:

The plaintext is encrypted as $c = \sum_{i=1}^{n} m_i \beta_i$.

Decryption Procedure:

$d \leftarrow c r^{-1} \mod q$
for $l = n$ **downto** 1 **do**
  if $d \ge w_l$ **then** $m_l \leftarrow 1$ **else** $m_l \leftarrow 0$ **end if**
  $d \leftarrow d - m_l w_l$
end for

(a) Show that $(\boldsymbol{w}, q, r) = ((2^0, 2^1, \ldots, 2^{n-1}), 2^n, 1)$ is a weak key in the sense that $m = c$.

Assume that $r \neq 1$ in the following.

(b) Show that $\beta_1, \ldots, \beta_n$ are pairwise different.

Alice encrypts two plaintexts $m \neq m'$ of the same length n with the same key $\boldsymbol{\beta}$ and obtains two different ciphertexts c and c'. A confidential source tells you that m and m' only differ in one bit position $1 \le j \le n$, i.e., $m_j \neq m'_j$ and $m_i = m'_i$ for all $i \neq j$.

(c) How can the bit position j be determined?

Bob encrypts a plaintext m of length $n = 5$. He chooses w_1 at random and uses the rules $w_i = 2w_{i-1} + 1$ for $i = 2, \ldots, n$ and $q = 257$. His public key is $\boldsymbol{\beta} = (168, 103, 230, 227, 221)$.

(d) Your confidential source provides $w_4 = 63$. Determine the secret key $(\boldsymbol{w}, q, r)$ for the given $\boldsymbol{\beta}$. **Hint**: $257 \cdot 7 - 31 \cdot 58 = 1$.

(e) Now, you receive the ciphertext $c = 846$. Compute m for the given values.

Exercise 3. Alice uses the RSA cryptosystem with public key $(n, e) = (4891, 1901)$ for signing.

(a) Compute the corresponding private key d.

(b) Generate the RSA signature $s = m^d \mod n$ for the message $m = 2013$.

In the following, a protocol for authentication of Alice (A) towards Bob (B) is given. It is based on an RSA system with public keys (n, e_A), (n, e_B) and private keys d_A, d_B.

1) B chooses a random number $2 \leq r < n$, calculates $r_A = r^{e_A} \mod n$ and sends r_A to A.
2) A calculates $r = {r_A}^{d_A} \mod n$ and $r_B = r^{e_B} \mod n$ and sends r_B to B.
3) B checks, if $r = {r_B}^{d_B} \mod n$ holds. If this is true, A is authenticated towards B.

Alice uses two different public keys ($e \neq e_A$) for signing and authentication. Oscar (O) does not know the private keys of Alice.

(c) How can Oscar impersonate Alice towards Bob?

(d) Why is Oscar not able to determine the random number r?

In the following, Alice utilizes the same public key ($e = e_A$) for both signing and authentication.

(e) Is it possible for Oscar to now determine the random number r? If so, how?

Exercise 4. Consider the cubic equation $E : y^2 = x^3 + 4x + 1$.

(a) Is E an elliptic curve over $\mathbb{F}_5$? Substantiate your answer.

(b) Determine all points on the elliptic curve E and the order of the corresponding group.

(c) Is point $Q = (1, 1)$ a generator of the group? Substantiate your answer.

In analogy to the *Square-and-Multiply* algorithm in a ring $\mathbb{Z}_n$, the k-th multiple of P can be algorithmically computed based on doubling and addition on an elliptic curve over a field $\mathbb{F}_q$. You may use the binary representation of factor $k = (k_m, \ldots, k_0)_2 = \sum_{i=0}^{m} k_i \, 2^i$.

(d) Describe $45P$ in terms of doubling and addition of P only.

(e) Formulate an *iterative Double-and-Add* algorithm $f_{\text{it}}(P, k)$ to calculate $k\,P$.

(f) Give a *recursive* version $f_{\text{rec}}(P, k)$ of the above *Double-and-Add* algorithm.