Homework 12 in Cryptography I

Prof. Dr. Rudolf Mathar, Michael Naehrig

28.01.2008

Exercise 34:

Consider the following cryptosystem. Message space $\mathcal{M}$, ciphertext space $\mathcal{C}$ and key space $\mathcal{K}$ all coincide with the space of bit sequences of length 8, i.e. $\mathcal{M} = \mathcal{C} = \mathcal{K} = \{0,1\}^8$.

A message $m = m_1m_2m_3m_4m_5m_6m_7m_8$ is encrypted with the key $k = k_1k_2k_3k_4k_5k_6k_7k_8$ as follows. First, message and key are divided into halves of 4 bits each:

$$m = L_0R_0, \ k = K_0K_1.$$

Encryption e now works in 2 rounds:

$$L_1 = R_0, R_1 = f(L_0, K_0),$$
$$L_2 = R_1, R_2 = f(L_1, K_1).$$

The cryptogram is $e(m,k) = c = L_2R_2$. The function $f : \{0,1\}^8 \to \{0,1\}^8$ which is used for encryption is defined as follows:

$$f(L_i, K_i) = S(L_i) \oplus K_i,$$

where S is the permutation cipher given by the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$.

(a) Show that the cryptosystem has perfect secrecy, if keys are chosen with equal probability.

Hint: First of all find a closed formula for e.

(b) Encrypt $m = 01011100$ with the key $k = 10010001$.

(c) Is it possible to use the same algorithm with a different key for decryption? If so, which key must be taken?

Exercise 35.
For primes p with $p \equiv 3 \pmod 4$ using Euler's criterium we have an efficient procedure, to compute square roots modulo p. For primes p with $p \equiv 5 \pmod 8$ there exists also a deterministic algorithm, to compute square roots modulo p:

Input: A prime p such that $p \equiv 5 \pmod 8$ and a quadratic residue a modulo p
Output: Both square roots of a modulo p
$d \leftarrow a^{\frac{p-1}{4}} \mod p$
if $(d = 1)$ **then**
$r \leftarrow a^{\frac{p+3}{8}} \mod p$
end if
if $(d = p - 1)$ **then**
$r \leftarrow 2a(4a)^{\frac{p-5}{8}} \mod p$
end if
return $(r, -r)$

a) Show, that 1 and $p - 1$ are the only values which d can assume.

b) Show, that the algorithm indeed computes both square roots of a modulo p, by using that 2 is a quadratic non-residue modulo p.

Exercise 36:

Alice's public RSA-key is $(n, e) = (4819, 2753)$. Sign the document m with hash $h(m) = 117$ in the name of Alice.

Exercise 37:
Bob's public ElGamal-key is $(p, a, y) = (101, 2, 11)$.

(a) Determine the plain text of the message $(c_1, c_2) = (64, 79)$ which was sent to Bob without computing Bob's private key.

(b) Now determine Bob's private ElGamal-key.

Exercise 38.

The RSA-system is based on the ring $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/(pq)\mathbb{Z}$ for two primes p and q. Describe, how RSA can be carried over to the ring $\mathbb{F}_2[X]/(fg)\mathbb{F}_2[X]$. For this let f and g be two irreducible polynomials in $\mathbb{F}_2[X]$ such that $\deg(f) + \deg(g) = 2048$.
Answer the following questions:

a) How can a message $m \in \{0, 1\}^{2048}$ be represented as an element of $\mathbb{F}_2[X]/(fg)\mathbb{F}_2[X]$?

b) How must public and private keys of a user A be chosen?

c) Determine the encryption and decryption functions?

Additionally answer the following question:

d) Does the constructed system have comparable security to RSA? Give reasons for your answer!

Hint: It holds $|(\mathbb{F}_2[X]/(fg)\mathbb{F}_2[X])^*| = (2^{\deg(f)} - 1)(2^{\deg(g)} - 1)$.