T-79.4501 Cryptography and Data Security (5 cr)
T-110.5210 Cryptosystems (5 cr)

Students of the course T-110.5210 Cryptosystems (4 cr): Give answers to at most four (4) problems. Please, mark clearly that your exam is for 4 credits only!

EXAM
Thursday, February 20, 2014

1. (6 pts) Consider an *Autokey cipher* in ring $\mathcal{R}$ with key b of length $m = 1$. Then given plaintext $x = (x_1, \ldots, x_n)$ the ciphertext $y = (y_1, \ldots, y_n)$ is computed as

$$\begin{aligned} y_1 &= x_1 + b \\ y_i &= x_i + x_{i-1}, \text{ for } i = 2, \ldots, n. \end{aligned}$$

The attacker sees the ciphertext, and transforms it to sequence $z = (z_1, \ldots, z_n)$ as follows:

$$\begin{aligned} z_1 &= y_1 \\ z_i &= y_i - z_{i-1}, \text{ for } i = 2, \ldots, n. \end{aligned}$$

Show that then z is equal to the ciphertext obtained by encrypting x using the 2-dimensional Vigenère cipher with keyword $(b, -b)$.

2. Consider the matrix

$$A = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix}$$

   (a) (2 pts) Show that A represents multiplication by an element α in the field $\mathbb{F} = \mathbb{F}_2[x]/\langle x^3 + x + 1 \rangle$, where $\alpha(x) = x + 1$

   (b) (2 pts) Calculate α^{-1} in $\mathbb{F}$ using the Extended Euclidean Algorithm.

   (c) (2 pts) Give A^{-1}. (Hint: A^{-1} represents multiplication by α^{-1} in $\mathbb{F}$.)

3. (a) (3 pts) Describe the operation of the Counter (CTR) mode of a block cipher.

   (b) (3 pts) Block cipher in CTR mode can be regarded as a stream cipher. What is the length of its period in bits?

4. Consider the RSA cryptosystem with modulus $n = 31 \cdot 43 = 1333$.

   (a) (3 pts) The random number generator returns two numbers 245 and 143. Which of them is suitable to be used as a private decryption exponent d?

   (b) (3 pts) Decrypt the ciphertext $c = 903$ with the help of the Chinese Remainder Theorem. That is, compute

$$\begin{aligned} m_1 &= c^d \bmod 31 \\ m_2 &= c^d \bmod 43 \end{aligned}$$

   and then use the Chinese Remainder Theorem to compute m such that

$$\begin{aligned} m_1 &= m \bmod 31 \\ m_2 &= m \bmod 43. \end{aligned}$$

5. (6 pts) The DSA signature is a pair (r, s), where

$$\begin{aligned} r &= (g^k \bmod p) \bmod q \\ s &= (h(m) + dr)k^{-1} \bmod q. \end{aligned}$$

Alice uses a toy version of the DSA signature scheme with a prime modulus $p = 43$ and generator $g = 21$ of order $q = 7$. By accident, Alice generates signatures for two different messages with the same per-message random number k. The hashes of the two signed messages are 2 and 3, and the signatures are (2, 1) and (2, 6), respectively. Compute Alice's private key without computing a discrete logarithm.

Exam Calculator Policy. It is allowed to use a function calculator, however no programmable calculator.