T-79.4502 Cryptography and Data Security (5 cr)
T-110.5210 Cryptosystems (5 cr)
December 20, 2012 / Exam

Students of the course **T-110.5210 Cryptosystems (4 cr)** give answers to at most four (4) problems. Clearly mark that your exam is for 4 credits only.

Each problem is worth 6 points. A non-programmable pocket calculator is allowed.

1. Consider the matrix

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

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

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

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

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

3. Consider a hash function h which uses AES encryption operation E_K with 128-bit key K as a compression function to compute the chaining value H_i as follows:

$$\begin{aligned} H_0 &= IV \\ H_i &= E_{M_i}(H_{i-1}), \text{ for } i = 1, 2, \ldots, \ell, \end{aligned}$$

   where IV is a fixed known 128-bit initial value, and the message M is presented as a sequence of ℓ blocks M_i of 128 bits each. As usual, we set $h(M) = H_\ell$. Given a hash value H show that it takes roughly about 2^{64} steps of computation and about the same amount of memory to find a message of two blocks $M = M_1 || M_2$ such that $h(M) = H$. Hint: Use meet-in-the-middle technique. Is h a good hash function?

4. (a) Find the smallest positive integer which is a primitive element in $\mathbf{F}_{17}^*$.

   (b) Find an element of order 8 in $\mathbf{F}_{17}^*$.

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

   (a) 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) 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

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

Feedback from students plays a vital role in improving this course. Please submit any feedback by following the link through the Noppa page.