T-79.4501 Cryptography and Data Security (5 cr)
T-110.5210 Cryptosystems (~~5~~ 4 cr)

EXAM
Thursday, March 10, 2011

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.

1. (6 pts) The key of *Hill cipher* is a 3×3 matrix

$$K = \begin{pmatrix} k_1 & k_2 & k_3 \\ k_4 & k_5 & k_6 \\ k_7 & k_8 & k_9 \end{pmatrix},$$

where the unknown $k_i \in \{0, 1, \ldots, 25\} = \{\mathtt{A}, \mathtt{B}, \ldots, \mathtt{Y}, \mathtt{Z}\}$ can be solved given a sufficient number (at least three are needed) known plaintext-ciphertext pairs. It is given that $E_K(\mathtt{sky}) = \mathtt{BAA}$, $E_K(\mathtt{sun}) = \mathtt{ABA}$, $E_K(\mathtt{hat}) = \mathtt{AAB}$. Find the decryption matrix, that is, the inverse K^{-1} of the key matrix K.

2. Describe by drawing a picture, or using formulas, or both
   (a) (2 pts) the encryption function of the CBC mode of operation;
   (b) (2 pts) the decryption function of the CBC mode of operation; and
   (c) (2 pts) the CBC MAC.

3. (6 pts) In the round key expansion procedure, AES uses 8-bit constants C_i, $i = 1, 2, 3, ..., 30$ that can be computed as

$$C_i = 2^{i-1}$$

in polynomial arithmetic modulo $m(x) = x^8 + x^4 + x^3 + x + 1$, that is, in Galois field $GF(2^8)$ with polynomial $m(x)$. Compute C_{11}, C_{12} and C_{22}.

4. (6 pts) Alice is using the RSA cryptosystem with modulus $N = 1003 = 17 \cdot 59$ and public exponent e, which is an odd integer. The plaintext is $x = 237$. Show that then the ciphertext is $y = 237$.

5. (6 pts) There are several variations to the DSS signature scheme. In the Nyberg-Rueppel variation the signature (r, s) is computed as

$$\begin{aligned} r &= (H \cdot (g^k \bmod p)) \bmod q \\ s &= (k - a \cdot r) \bmod q \,. \end{aligned}$$

When generating the signature, the signer checks that $(g^k \bmod p) \bmod q \neq 0$. The private key is $a \in \mathbb{Z}_q$ and the public key is $V = g^a \bmod p$.

Show how the hash code H, $0 < H < q$, can be recovered from the signature (r, s) using public information only. (Hint: Recover the exponential $g^k \bmod p$ first.)

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