4502

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, March 8, 2012

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. Alice and Bob use CBC encryption. The plaintext is a sequence of blocks $P_1, P_2, \ldots, P_t$ and the corresponding ciphertext blocks sent by Alice to Bob are $C_1, C_2, \ldots, C_t$. Bob receives ciphertext blocks $C'_1, C'_2, \ldots, C'_t$, where exactly one ciphertext block C'_j has an error, where $1 \leq j < t$. Then $C'_i = C_i$ for all $i = 1, 2, \ldots, t$, $i \neq j$, and $C'_j \neq C_j$.

   a) (3 pts) Show that after decryption by Bob exactly two plaintext blocks are erroneous. What are the indices of the erroneous plaintext blocks?

   b) (3 pts) How do the erroneous plaintext blocks differ from the original?

3. (6 pts) Consider polynomial arithmetic in the set of 3-bit integers using polynomial $x^3 + x + 1$.

   (a) (3 pts) Determine the discrete logarithm of $6 = \mathtt{110}$ to the base $2 = \mathtt{010}$.

   (b) (3 pts) Calculate the inverse of $6 = \mathtt{110}$.

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) Assume that we have two number generators as black boxes. Both generators output 64-bit numbers. One box contains a Counter Mode PRNG using Triple-DES encryption as E_K and with a counter of length 64 bits. The second box contains a true random number generator. The boxes look exactly the same, and the task is to determine which one is the true RNG just by examining the output of the generators. After both generators have produced more than about 2^{32} numbers, one has more than 50% chance of being able to distinguish the generators. Explain why.

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