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
Wednesday, December 18, 2013

1. (6 pts) Let us consider a stream cipher defined as follows:

$$\begin{aligned}\mathcal{P}=\mathcal{C} &= \mathbb{Z}_7^8,\\ \mathcal{K} &= \{(a,b)\,|\,\gcd(a,7)=1\}\\ z_i &= (a\cdot i+b) \bmod 7,\ i=1,2,\ldots,8,\ \text{where } (a,b)\in\mathcal{K}\\ e_K(x) &= y=(y_1,y_2,\ldots,y_8),\ \text{where } x=(x_1,x_2,\ldots,x_8),\ K=(a,b)\in\mathcal{K},\ \text{and}\\ y_i &= (x_i+z_i) \bmod 7,\ \text{for } i=1,2,\ldots,8.\end{aligned}$$

   (a) Using (5,3) as the key, compute the decryption of the message 25542531.

   (b) If you know that some part of the plaintext is 10503, and the corresponding part of the ciphertext is 01153, then derive as much as you can about the unknown key (a,b). What additional information you need to derive the entire key?

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

   (a) (3 pts) Determine the discrete logarithm of $x^2 + x = \texttt{110}$ to the base $x = \texttt{010}$.

   (b) (3 pts) Calculate the inverse of $x^2 + x = \texttt{110}$.

4. Consider the matrix

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

   (a) (3 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 $\alpha(x) = x^2 + x$

   (b) (3 pts) Give A^{-1}. (Hint: A^{-1} represents multiplication by α^{-1} in $\mathbb{F}$.)

5. (6 pts) Alice is using a toy version of the DSA signature scheme with a prime modulus $p = 47$ and generator $g = 2$ of order $q = 23$. By accident, Alice generates signatures for two different messages with the same random number k. The hash codes of the two signed messages are 2 and 3 and the signatures are (4, 21) and (4, 19), 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.

Course Feedback. You are kindly reminded to give course feedback at
`http://www.cse.tkk.fi/cgi-bin/teekysely.pl?action=showform&id=T794502-T794502-s2013palaute&lang=ENG`
or using the link given in Noppa.