CS-E4320 Cryptography and Data Security (5 cr)

EXAM
Thursday, February 16, 2017

Each problem is worth 6 points. This is a 30 point exam.

1. (6 pts)
   (a) (3 pts) A ciphertext has been generated with an affine cipher. The most frequent letter of the ciphertext is "B" and the second most frequent letter of the ciphertext is "U". Knowing that the plaintext was an English text, explain how to find the encryption key.
   (b) (3 pts) Draw and describe a Substitution-Permutation network. Explain its use in block cipher design. Name one block cipher that uses this construction.

2. (6 pts) 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)
   (a) (3 pts) Solve the equation $5x = 1 \pmod{31}$.
   (b) (3 pts) Use the CRT to solve the following system.

$$\begin{cases} x = 15 & (\text{mod } 31) \\ x = 8 & (\text{mod } 7) \end{cases}$$

4. (a) (3 pts) Consider the RSA cryptosystem with modulus $n = 31 \cdot 43 = 1333$. The random number generator returns two numbers 301 and 311. Which of them is suitable to be used as a private decryption exponent d? Using this private exponent, decrypt the ciphertext $c = 993$.
   (b) (3 pts) An instance of square-and-multiply algorithm computation has the following 8 steps

i	y
7	$993^2 \bmod 1333 = 962$
6	$962^2 \bmod 1333 = 342$
5	$342^2 \cdot 993 \bmod 1333 = 962$
4	$962^2 \cdot 993 \bmod 1333 = 1024$
3	$1024^2 \bmod 1333 = 838$
2	$838^2 \bmod 1333 = 1086$
1	$1086^2 \cdot 993 \bmod 1333 = 1086$
0	$1086^2 \bmod 1333 = 1024$

   Using this information, find an integer d such that $993^d \bmod 1333 = 1024$.

5. (6 pts) Alice and Bob use the Diffie-Hellman key exchange technique with a common prime $p = 17$ and a primitive root $g = 7$.
   (a) (4 pts) If Alice has private key $X_A = 3$, what is the public key (Y_A) of Alice?
   (b) (2 pts) Knowing that the public key of Bob is $Y_B = 4$, what is the shared secret key?

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