TU Delft

Delft University of Technology
Faculty of Electrical Engineering, Mathematics, and Computer Science
Department of Mediamatics
Information Security and Privacy Lab

SECURITY AND CRYPTOGRAPHY (IN4191)
CRYPTOGRAPHY (ET4271)

Exam, June 22, 2010

Important:
This exam exists out of 4 questions. Write the answers for each question on a separate sheet of paper. This is necessary because for correction the questions are separated. Do not forget to put your name and student number on every sheet of paper.

Question 1: Key management/ RSA (10 points)

Suppose Alice wants to send Bob a secret message by using a hybrid scheme described below.

Hybrid scheme: First a session key (J) is generated and a message (M) is encrypted by using the symmetric scheme E(M, J) = (M + J) mod 256. Secondly, the session key is encrypted by using the RSA cryptosystem. Finally, both values – ciphertext and encrypted session key – are sent to the other involved entity.

From here, suppose that the public key of Alice and Bob is given by $(e_A, n_A) = (5, 69)$ and $(e_B, n_B) = (7, 65)$, respectively.

1) Suppose Alice generates the session key by selecting the first six bits provided by a Linear Feed Back Polynomial (LFSR). The LFSR is set by $f(x) = x^3 + x^2 +1$ feed-back function and the initial state is 101. Compute the session key (J) generated by Alice. (3 points)

2) Ignore the result of 1) and assume $J = 111001_2 = 57_{10}$ and M = 218. Compute the ciphertext and encrypted session key that Alice sends to Bob by using the hybrid scheme described previously. (3 points)

3) Ignore the result of 2) and assume that Alice sends to Bob the pair of values (8, 9), which represents the symmetric encryption of message (M) and the

asymmetric encryption of session key (J), respectively. Compute the operations executed by Bob to decipher the message received. (4 points)

Note: 57^2 mod 69 = 6

Question 2: Authentication/ DES (10 points)

Alice and Bob are using the DES-algorithm in the CBC-mode (Cipher Block Chaining mode) for both encryption and message authentication.

a) Draw the scheme of the CBC-mode for encryption. (1 point)

b) In the case of encryption in the CBC-mode one sometimes uses an extra Initial Vector (IV) if the first block is encrypted. Give two advantages for the usage of this IV (max. 4 lines). (2 points)

c) Assume that during transmission the ciphertext blocks 2, 4 and 7 are changed by the occurrence of bit errors. Which blocks will be decrypted incorrectly at the receiver? Give a short elucidation. (2 points)

d) Similar question as c). But now the ciphertext blocks 2, 4 and 7 are 'missing blocks'. I.e. they have not been received at all by the receiver. (2 points)

e) Draw the scheme for using DES in aid of message authentication. (1 point)

f) In order to avoid complex key management one decides to use the same DES-key for both encryption and message authentication. Is this a good idea (explain in max. 5 lines)? Hint: Consider what happens if two different keys are used and the key for encryption is compromised. (2 points)

Question 3: Diffie-Hellmann (10 points)

Alice and Bob plan to communicate in a secret way. For this purpose, they decide to create a key using Diffie-Hellman key exchange scheme. Therefore, Alice and Bob choose a prime number *p* and a generator *g*. Alice and Bob pick random values r_1 and r_2, respectively. Then, Alice sends Bob g^{r1} mod p and Bob send Alice g^{r2} mod p. Alice can obtain the key by computing $(g^{r2})^{r1}$ mod p and Bob can obtain the key by computing $(g^{r1})^{r2}$ mod p.

a) For p=11, show that g=2 is a generator and g=3 is not a generator. (A generator is a primitive element whose powers generate the set {1, 2, 3, 4, 5, 6, 7, 8, 9, 10} for p=11.) (2 points)
b) Explain why this scheme is difficult to break. What happens if Alice and Bob chose a *g* which is not a generator? (2 points)
c) For p=11 and g=2, generate a key for Alice and Bob. (3 points)

d) Alice has a secret key y such that y=a^x mod p. Distribute this secret key to 3 trusted third parties (TTP1, TTP2 and TTP3) by using Fair Diffie-Hellman cryptosystem. Explain what a fair cryptosystem is. Explain why any attempt by one or two TTPs is futile for obtaining the secret key of Alice. (3 points)

Question 4: Information theoretical approach (10 points)

Assume M denotes the plaintext, C the ciphertext and K the key.

a) Proof the following:

$$H(M/C) = H(K/C) - H(K/M,C).\ \text{(2 points)}$$

b) Explain what is meant with the term "cryptographic dilemma", which is represented by the equation given in a) (1 point)

c) Take now into account the length L of both the plaintexts and ciphertexts. It holds that $H(K)$=20 and that $H(K/M^L,C^L)$ is linear function such that $H(K/M^L,C^L)$=0 for L=10. Furthermore, it holds that $H(M^L/C^L)$=0 for L=100, achieves a maximum (which is equal to 10) for L=10 and consists of two linear functions. Sketch in one figure $H(M^L/C^L)$ and $H(K/M^L,C^L)$ as functions of L. (2 points)

d) Give for the conditions mentioned in c), the equation for $H(K/C^L)$ as a function of L and draw it in the same figure as that of c). (2 points)

e) Proof that:

$$I(M;C) \geq H(M) - H(K).\ \text{(2 points)}$$

f) Consider the equation given in e). What can you say about the minimum number of keys in order to guarantee absolute security in the cases that all plaintexts are equiprobable? (1 point)