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)

Exam, April 6, 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 : Zero-knowledge (10 points)
Alice wants to proof her identity to Bob by means of a zero-knowledge protocol. Alice owns two secret numbers (s_1,s_2), which satisfy $s_i^2 v_i=1 \pmod n$, i=1,2. She chooses two random numbers r_j and computes $x_j=r_j^2 \pmod n$, j=1,2 and sends these to Bob. Bob sends a 2x2 matrix T with binary elements t_{ji} to Alice. Alice computes $y_j=r_j s_1^{t_{j1}} s_2^{t_{j2}} \pmod n$, j=1,2 and sends them to Bob.

a) Give the computations which Bob should perform to verify Alice's identity. (2 points)
b) Explain (max. 50 words) why it is difficult for attacker Charles to pretend to be Alice. (1 point)

Let n=143, $(s_1,s_2)=(7,3)$, $(r_1,r_2)=(16,20)$ and T is given by two rows (1,1) above and (0,1) below.

c) Compute (v_1,v_2). (2 points)
d) Compute the pairs (x_1,x_2) and (y_1,y_2) that Alice sends to Bob. (2 points)
e) Perform the computations of Bob when he verifies Alice's identity. (2 points)
f) What is the probability that Bob can pretend to be Alice. (1 point)

Question 2: Shift registers (10 points)
To generate a pseudo-random value to be used as a key for encryption, a LFSR with $f(x)=1+x+x^3$ is selected with initial state (0,1,0).

a) Show in a table the states of the registers and the output for the first 10 clock cycles. (1 point)
b) What is the period of this LFSR? Does it have the maximal length? Justify your answer by using polynomial approach. (2 points)

c) Consider the bits for the first period. Does this sequence satisfy the postulates of Golomb? (2 points)

Consider that a ten bit message M=(1110010010) is encrypted by using the LFSR system above. (The first bit of the message is the bit '0'.)

d) What is the ciphertext? (1 point)

e) Assume that the third bit of the ciphertext is received with error. What is the decrypted message? (1 point)

f) Assume that the third bit of the ciphertext is NOT received. What is the decrypted message? (1 point)

g) What is the number of characteristic polynomials with maximal length for a LFSR with 6 registers. (2 points)

Question 3: Secret Sharing (10 points)

Alice, Bob, Carol and David want to share an 8-bit secret key which is given by (01101011).

a) The key is broken up in four parts. Alice's share is (01), the share of Bob is (10) et cetera. How many potential keys an attacker should try in case he has no or just one share, respectively. Mention two disadvantages of this secret sharing scheme.

b) Instead of the method given in a) now dual control is applied. The shares of Alice, Bob and Carol are (11100101), (00101010) and (11100011), respectively. What is the share of David? And how many keys an attacker should try in case that he has one or two shares?

Alice, Bob and Carol now want to share a secret number s. They want a dual control based system that reveals this secret number to any two of the three players. For Alice, Bob and Carol three different share pairs for s are created, giving the three sets of two shares to Alice and Bob, Alice and Carol, and Bob and Carol. The shares of set 1 of Alice and Bob are 3 and 42, respectively. In set 2 the share of Carol is 12 and in set 3 the share of Bob is given by 23.

c) Give the values of the missing shares as well as the secret value s.

Now David joins the party and they now want that any three of the four players can find the secret.

d) How many sets of shares are needed? How many shares are in each set?

e) What is the number of sets if any t of n players should reveal the secret s? What is the drawback of this system?

Assume that Alice, Bob, Carol and David use Shamir's (t,n) Threshold Scheme, with t=3. The function that generates the shares is given by $f(x)=7x^2+8x+12 \pmod{13}$.

f) Compute the shares of Alice, Bob, Carol and David. What is the secret?

Question 4: S-DES (10 points)

The simplified DES encryption algorithm (S-DES) takes an 8-bit block of plaintext and a 10-bit key as input and produces an 8-bit block of ciphertext as output.

The encryption algorithm involves five functions: 1) an initial permutation (IP); 2) a complex function labeled f_k, which involves both permutation and substitution

operations and depends on a key input; 3) a simple permutation function that switches (SW) the two halves of the data; 4) the function f_k again; 5) a permutation function that is the inverse of the initial permutation.

The function f_k

The function can be expressed as follows. Let *L* and *R* be the leftmost 4 bits and rightmost 4 bits of the 8-bit input to f_k, and let F be a mapping (not necessarily one to one) from 4-bit strings to 4-bit strings. Then we let

$$f_k(L, R) = (L \oplus F(R, k_i), R).$$

where k_i is a subkey and $\oplus$ is the bit-by-bit exclusive-OR function.

We now describe the mapping F. The rightmost 4 bits (R) of the 8-bit input to f_k are the inputs of an expansion/permutation operation (EP). Then, the 8-bit subkey k_i is xored with the output of the EP operation. From the 8-bit resulting, the leftmost 4 bits are fed into the S-box S0 to produce a 2-bit output, and the remaining 4 bits are fed into S1 to produce another 2-bit output. The S-boxes operate as follows. The first and fourth input bits are treated as a 2-bit number that specify a row of the S-box, and the second and third input bits specify a column of the S-box. The entry in that row and column, in base 2, is the 2-bit output. Next, the 4 bits produced by S0 and S1 undergo a further permutation (P4) and its result represents the output of f_k function.

Key generation (k_1, k_2)

S-DES depends on the use of a 10-bit key shared between sender and receiver. From this key, two 8-bit subkeys are produced. We now describe the specific steps. First, the initial key is permuted by using P10. Next, the output is divided into two halves of five bits and we perform a circular left shift (LS-1), or rotation, in each of them. The 10-bits obtained are the input of a compression/permutation operation (P8). The result is the subkey k_1. We then go back to the pair of 5-bit strings produced by the two LS-1 functions and we perform a circular left shift of 2 bit positions on each string (LS-2). Finally, P8 is applied again to produce k_2.

a) Let K = 1010000010, compute k_1 and k_2. (3 points)

b) Assuming that we use S-DES block cipher in CBC mode, depict in a figure the resulting cryptosystem (without giving the details of S-DES). (2 points)

c) Let the subkeys k_1= 01011011 and k_2= 10111100 and the plain text M=01110011 01101111, compute the ciphertext if CBC mode is used and initial vector IV= 01100001. (5 points)

S0

1	0	3	2
3	2	1	0
0	2	1	3
3	1	3	2

S1

0	1	2	3
2	0	1	3
3	0	1	0
2	1	0	3

P10

3	5	2	7	4	10	1	9	8	6

P8

6	3	7	4	8	5	10	9

P4

2	4	3	1

IP

2	6	3	1	4	8	5	7

IP^{-1}

4	1	3	5	7	2	8	6

EP

4	1	2	3	2	3	4	1