Delft University of Technology
Faculty of Electrical Engineering, Mathematics, and Computer Science
Department of Intelligent Systems
Cyber Security Group

CRYPTOGRAPHY (IN4191)
19-01-2016
13:30-16:30

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.

REMARK: DO NOT FORGET TO WRITE DOWN YOUR NAME and STUDENT NUMBER ON EACH SHEET IN a READABLE FORM!

Make it clear in your answers how you reach the final result; the road to the answer is very important.

It is allowed to answer in Dutch or English.

Question 1: Elliptic Curve Diffie-Hellman (10 pts)
Using the Deffie-Hellman protocol for key exchange makes it possible for Alice and Bob to generate a secret key K. Alice and Bob each have a piece of secret and some mutual information. Usually, this protocol is based on exponential and logarithmic functions but it can be represented with elliptical curves.

Alice generates for following elliptic curve:

$$E : y^2 = x^3 + 2x + 2 \pmod{11}$$

Having chosen a point $P = (1,4) \in E$, it is sent together with the elliptic curve to Bob. Alice also chooses a random natural number $c = 2$.

a) Compute cP. (2 pts)

Formulas for computing $R = P + Q$

$P = (x_1, y_1), Q = (x_2, y_2), R = (x_3, y_3)$

$x_3 = \sigma^2 - x_1 - x_2 \pmod{p}$

$y_3 = \sigma(x_1 - x_3) - y_1 \pmod{p}$

$\sigma = \frac{y_2 - y_1}{x_2 - x_1}$ if $P \neq Q$

$\sigma = \frac{3x_1^2 + 2}{2y_1}$ if $P = Q$

Note: $\frac{a}{b} \pmod p = ab^{-1} \pmod p$, where b^{-1} is inverse of b in $(\bmod\, p)$.

To compute the secret key K, Alice and Bob have to compute the following protocol:

- Bob chooses a random number $d = 3$ and computes $dP = 3P = (9,10) \in E$.
- Alice receives dP from Bob.
- She is now able to compute the secret key K by computing $K = cdP = (9,1)$.

b) What should Bob do after Alice had sent him cP and they want to have a secure computation? (1 pts)

An eavesdropper Eve still can perform a man-in-the-middle attack on the communication between Alice and Bob.

c) Describe in maximum 50 words how Eve can eavesdrop on communication of Alice and Bob without being noticed. (2 pts)

After finishing the protocol Alice and Bob both share the same secret key K. Now they want to send this symmetric key to a Trusted Third Party (TTP) using an elliptic-curve based public-key encryption scheme with the public key (Q, P) of the TTP, where $Q = \alpha P$.

Alice sends the message $M = K = (9,1)$ to the TTP. She uses the above elliptic curve E which has 9 points in the elliptic group.

Alice holds the following: $Q = (5,4), k = 2, P = (1,4), p = 11, \alpha = 4$

d) Compute kQ. (2 pts)

e) Compute the ciphertext C using the EL-Gamal system. (3 pts)

Question 2: Secret Sharing (10 pts)

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. (2 pts)

b) Instead of 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 he has one or two shares? (2 pts)

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 missing shares as well as the secret value s. (1 pts)

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? (1 pts)

e) What is the number of sets if any t of n players should reveal the secret key s? What is drawback of this system? (2 pts)

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? (2 pts)

Question 3: Authentication (10 points)
For authentication between Alice and Bob there are various methods, e.g. challenge-response methods based on symmetrical algorithms, Message Authentication Codes (MAC's), digital signature based on asymmetrical algorithms, zero-knowledge techniques et cetera.

a) Mention one advantage and one disadvantage of zero-knowledge techniques in comparison with other authentication methods? (max. 30 words) (2 pts)

b) Give the scheme of three-way challenge-response between Alice and Bob based on a symmetrical algorithm. (2 pts)

c) Give the scheme for message authentication between Alice and Bob with the help of a MAC. (2 pts)

d) Give the scheme for how a MAC can be generated with the help of DES. (1 pts)

e) Give the scheme for the generation of a digital signature generated by Bob on the basis of RSA, when he wants to send a signed and encrypted message to Alice. (2 pts)

f) What is the reason that in practice a digital signature with the help of RSA is not performed on the message itself, but on the hash-value of the message? (max. 30 words.) (1 pts)

Question 4: Shift Register (10 points)

Alice wants to send Bob confidential data. For this purpose, Alice decides to use the following encryption scheme: $E(m) = m \oplus r$, where m is a binary message and r is a random value.

a) Alice uses an LFSR with 3 registers to generate the random value. Assuming that the first and the third registers are tapped and initial state is (101), draw a diagram and give the output of this shift register for the first 7 bits. Prove that this value is pseudo-random, or not, using the Golomb's postulates. (4 pts)

b) Explain two advantages and two disadvantages of using this encryption scheme in real world. (2 pts)

c) Bob receives the encryption $m \oplus r$, however he is not sure about the origin of the message. What should Bob do to convince that the message is originating from her? Explain your answer. (2 pts)

d) For Charles eavesdropping the message, it is easy to modify/destroy the message by xor-ing the message with another bit string. What should Alice do so that Bob can check whether the message is intact? (2 pts)