Delft University of Technology
Faculty of Electrical Engineering, Mathematics, and Computer Science
Department of Mediamatics
Information and Communication Theory Group

CRYPTOGRAPHY (ET4271)

Exam, Monday July 2, 2007, 14.00 - 17.00

Belangrijk:
Dit tentamen bestaat uit 4 opgaven. Aangezien het tentamen bij het nakijken wordt uitgesplitst per opgave, dient u elke opgave op een nieuw vel papier te beginnen. Vergeet vooral niet om elk vel van uw naam en studienummer te voorzien! Dit tentamen is in het Engels. Als er problemen zijn met het begrijpen van de Engelse vraagstelling, aarzel dan niet om hulp te vragen aan de surveillanten.

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

Question 1.

Using the Diffie-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 also be done by using with elliptical curves.

Alice generates the following elliptic curve:

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

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

Formulas for computing $R = P + Q$

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

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

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

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

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

a) Compute cP

To compute the secret key K, Alice and Bob perform 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 be done by Bob to derive the shared secret key K such that he shares the same key as Alice?

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 the communication of Alice and Bob without being noticed.

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: $Q = (5,4), k = 2, P = (1,4), p = 11, a = 4$

d) Compute kQ.

e) Compute the ciphertext C using the Elgamal system.

f) Compute the ciphertext C using the Menezes-Vanstone system.

New separate sheet of paper!

Question 2.

Data security is a possible application of the RSA algorithm, which is initiated by generating keys based on two prime numbers p and q. The numbers e and d, which are based on the two generated prime numbers, play a major role in the encryption and decryption of messages, respectively.

a) Let M be the original message. Give the formulas for encryption and decryption of the message M. Indicate in these formulas the public key.

b) Give the Euler totient function and show by using the Euler totient function that the encryption and decryption operation of RSA is each other's inverse.

From here it holds that: $p=5$, $q=17$ and $e=11$

c) Compute d with the help of the Euclidian algorithm.

d) Let $C=68$ be the encrypted message. Compute M.

e) The RSA algorithm can also be used to generate digital signatures. Student lansen transforms each letter of his first name into a number corresponding to the position in the alphabet ($A=1$, $B=2$ etc.). Then he generates a digital signature, which results in (40, 64). Give the first name of student lansen and provide the corresponding computation.

f) Draw the scheme where the on RSA based digital signature is combined with encryption and make sure that the message M is hashed and then digital signed. Show both the transmitting and the receiving side.

New separate sheet of paper!

Question 3.

a) Give the three postulates of Golomb for pseudo-random sequences.

b) Determine if the following sequence with period 15 satisfies the postulates of Golomb:

$$1\,0\,1\,1\,1\,1\,0\,0\,1\,1\,0\,0\,0\,1\,0$$

c) Construct the linear feedback shift register with minimum number of sections that generates the sequence 1000111101.1

d) Give a scheme that shows how the output of a shift register can be used to encrypt bit streams. Will this system be a perfect secure cryptosystem?

e) Explain in maximum 30 words what a "chosen-plaintext attack" is? What is the minimum plaintext size, of the in c) constructed shift register, to be able to have a successful chosen-plaintext attack?

New separate sheet of paper!

Question 4.

When we use key management with symmetric algorithms we can distinguish between two different systems namely on-line key distribution and off-line key distribution.

a) What is the advantage of on-line key distribution compared to off-line key distribution?

Alice and Bob want to communicate with each other by using an on-line key distribution protocol. One of the solutions to provide on-line key distribution is using a so-called hierarchical key system.

b) Explain what a hierarchical key system is and give and example of such a system?

Keys and Data are usually distributed and transported over networks. A characteristic of network communication is that data normally travels via several nodes, rather than following the most direct route between two parties. One of the methods of circulating data within a network is called end-to-end encipherment.

c) Name two other methods of circulating data within networks?

d) Draw the scheme of end-to-end encipherment.

e) What is the advantage of using the end-to-end encipherment compared to the other methods of circulating data within networks?

New separate sheet of paper!