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

CRYPTOGRAPHY (ET4271)

Exam, Wednesday April 1, 2009, 14.00 - 17.00

Question 1.

Let F be an elliptic curve. P=(x1,y1) and Q=(x2,y2) are points on the elliptic curve F and are public. The relation between P and Q is given by Q=aP, whereby a is secret. For encryption the El-Gamal cipher system is used.

a) What is the advantage of the El-Gamal system in comparison with RSA? Mention at least two advantages of he El-Gamal system.

b) Mention at least two disadvantages of the El-Gamal system.

In the El-Gamal system in addition to P, Q and a, also a random number k plays a role.

c) If the message that should be encrypted is given by M=(u1,u2), give the formula for the ciphertext C in terms of M, P, Q, a and k.

Let us assume that for a specific elliptic curve the formula's for the computation of (x3,y3)=R+S are given by:

$X3=\sigma^2 - x1 - x2 \pmod p$
$Y3=\sigma(x1 - x3) - y1 \pmod p$
$\sigma=(y2-y1)/(x2-x1)$, if $R\neq S$
$\sigma=(3\, x1^2 + 5)/(2\, y1)$, if R=S

Now the following holds: p=17, P=(3,5), a=3, k=2, M=(2,7)

d) Compute Q, as well as kP and kQ.

e) Compute the ciphertext C in the case of the El-Gamal system.

New separate sheet of paper!

Question 2.

A space research center, where highly secret research is performed, decides to introduce a system for access control (entity authentication) at the entrance gate.

a) There are two possibilities: two-way challenge-response or usage of a zeroknowledge technique. Which one do you prefer? Elucidate your answer and give arguments for your choice in at most 6 lines.

Assume now that a two-way challenge response is used.

b) Give the general scheme for a two-way challenge response.

In order to enable a practical implementation of a two-way challenge response it is assumed that each employee has a smartcard, and that there is a smartcard reader at the entrance gate.

c) Consider how the two-way challenge-response works in practice. Where the keys are stored? What computations should be performed in the smartcard and which ones in the smartcard reader? Since there are many employees in the space center, how does the smartcard reader knows that it uses the correct key in order to verify the response?

In stead of a two way challenge-response also a three way challenge-response could be used.

d) Give the general scheme of a three way challenge-response which is secure against a so-called reflection attack.

e) Taking into account the case of the space research center, would it be better to use a two- or a three-way challenge-response? Elucidate your answer in at most 6 lines.

New separate sheet of paper!

Question 3.

a) Give a mathematical formula for the unicity distance UD and elucidate the meaning of the used parameters in this formula.

b) Give at least two assumptions that underlie this formula?

Now assume a memoryless source with alphabet A=(a1,...,a8). For the probabilities p(a1),..., p(a7) it holds that: p(ai) = 2^{-i}

c) Compute UD in the case that the output of the source is encrypted with the help of a substitution cipher.

d) Compute UD in the case that two output symbols are put together to a new symbol and that these new symbols are encrypted with a substitution cipher. Explain in at most two lines the difference with the value of UD found in (c).

e) Discuss shortly whether the formula of UD given in (a) also holds for the case that a transposition cipher was used instead of a substitution cipher?

New separate sheet of paper!

Question 4.

The Dutch Ministry of Foreign Affairs wants to secure the communication with its various Dutch Embassies abroad by using the Rijndael-algorithm. The Rijndael-key (192 bits) is generated at the Ministry by co-operation of three employees; each of them generates a part of the key, the so-called subkeys.

a) Explain briefly (max. 5 lines) what the main advantage is of key-generation by three employees instead of by just one person.

In general there are two methods for the key generation:
Method 1: Each employee generates 192 bits. The final key is the result of the X-or addition of the three 192-bit subkeys within a tamper proof module.
Method 2: Each employee generates 64 bits. The final key is the result of concatenation of the three 64-bit subkeys within a tamper proof module.

b) Which method do you prefer from a security point of view, in the case that all subkeys are kept secret? Method 1 or Method 2? Elucidate your answer in at most 5 lines.

c) If one of the subkeys has been compromised, what is the maximum number of keys that should be tried by an intruder for each of the methods in the case of an 'exhaustive key search'?

Assume that the 192-bits Rijndael-key can be represented by the number 25. For the distribution of this Rijndael-key to the Embassies, the Ministry of Foreign Affairs now uses RSA. The public key of the Ministry is given by $e=13$, whereas the used primes are given by $p = 37$ and $q = 19$. For one of the Embassies e, p and q are given by 17, 89 and 11, respectively.

d) Compute the secret key of the Embassy.

e) Compute the ciphertext (= the enciphered Rijndael-key), which is sent by the Ministry to the Embassy.

Assume now, that in addition to encryption of the Rijndael-key also a digital signature is used.

Compute the ciphertext, which now is sent by the Ministry to the Embassy. Show your computations.