Delft University of Technology
Faculty EEMCS
Dept. Intelligent Systems
Information Security and Privacy Lab

Security and Cryptography (IN4191)

Exam, April 18, 2013, 14:00-17:00

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.

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

a) (3 pt) Explain additively homomorphic encryption briefly. Given two encrypted messages $E(m_1)$ and $E(m_2)$, show how to compute $E(2m_1 + 5m_2)$, assuming that the homomorphic operation is multiplication.

b) (3 pt) In a community with N people, what is the total number of keys if everyone wants to communicate with everyone else using a) AES and b) RSA. Compute the number of bits to store in each case, when AES-256 and RSA-1024 are chosen to be used.

c) (2 pt) Write down 2 advantages and 2 disadvantages of Elliptic Curve Cryptography.

d) (2 pt) Explain why a man in the middle attack works or does not work in quantum cryptography.

Question 2

Alice wants to convince Bob that she really is Alice. For that very reason they use a challenge-response protocol on the basis of a symmetric algorithm like AES.

a) (1 pt) Give a scheme that shows how this can be done, whereby at the same time the protocol is secure against a man-in-the-middle-attack. Instead of a challenge-response protocol, it was also possible to use a zero-knowledge protocol.

b) (2 pt) Mention at least one advantage and one disadvantage of a zero-knowledge protocol opposite to a challenge-response protocol on the basis of AES. In the initialization phase of a zero-knowledge protocol an independent third party generates for Alice a large number n, which is the product of two large primes p and q. It also generates for Alice an integer v which is a function of Alice's personal data and computes the secret value of s such that $s^2 v = 1 \bmod n$.

c) (1 pt) Give a method how v can be derived from Alice's personal data, like her account-number, Sofi-number, address et cetera. Assume now $p = 11$, $q = 13$ and $s = 7$.

d) (2 pt) Compute the original value of v **by using the Euclidean algorithm.** According to the protocol Alice sends a value x to Bob which is a function of a random number r selected by Alice. Bob answers by sending to Alice a binary value t which is equal to 0 or 1. Alice sends Bob a value y which is based on the value t among others and which y Bob needs for the verification step. Let $r = 5$.

e) (2 pt) Compute the values of y if $t = 0$ and $t = 1$, respectively.

f) (2 pt) What is the probability that an intruder Charles can pose as Alice if Bob performs just one check. How many checks Bob should do at least in order to be certain about the identity of Alice with 99%?

Question 3

The RSA cryptosystem is defined as follows. For a message $m \in \mathbb{Z}_n$,

$$E(m) = m^e \bmod n ,$$

where $n = p \cdot q$. The decryption function is:

$$D(c) = c^d \bmod n ,$$

where $ed = 1 \bmod \Phi(n)$ and $\Phi(n) = (p-1)(q-1)$.

For $p = 7$, $q = 11$ and $e = 13$,

a) (2 pt) compute d using the extended Euclidean algorithm.

b) (2 pt) compute the ciphertext c of the message $m = 15$.

c) (2 pt) compute the decryption of the ciphertext $c = 10$.

d) Assume that a file of 200 KB (kilobytes) is to be encrypted. There are two choices for the encryption scheme to use: AES with a key size of 256 bits, and RSA with a key size of 1024 bits. (1 KB = 1024 × 8 bits.)

   A) (1 pt) Compute the number of encryptions required to encrypt the file if AES is used.

   B) (1 pt) Compute the number of encryptions required to encrypt the file if RSA is used.

C) (2 pt) Compute the amount of data to be transmitted in KB if the file is encrypted using AES-256 and the encryption key is encrypted using RSA-1024. (That is the total size of the encrypted file and encrypted 'key'.)

e) (2 pt) Explain probabilistic encryption using the Paillier cryptosystem as an example. Modify AES to be probabilistic. (Encryption function in the Paillier cryptosytem: $E(m) = g^m r^n \bmod n^2$.)

Question 4

Alice should give her DNA but she likes to protect her privacy. For that very reason she gives partial information about her DNA to three different parties. Her DNA is CCTGATAGC. The first three symbols are given to the first party, the second three symbols to the second party et cetera.

a) (1 pt) The first party is the bad guy. How much effort he should do in order to reconstruct the whole DNA by means of an exhaustive search?

b) (2 pt) Another approach is giving to two parties each a random DNA. What should be given to the third party such that together they can reconstruct the original DNA (Hint: take two random DNA sequences of length 9 and determine the third sequence for the third party). Elucidate the method which you propose.

c) (1 pt) In case of b) assume the first party is again the bad guy. What is now the effort he has to do in order to reconstruct the original DNA sequence?

Assume the maximum length (L) of a sequence of identical bases (e.g. CCCCC) in the whole DNA sequence is highly sensitive information. This number is shared by means of a (t, n) secret sharing scheme.

d) (1 pt) Explain why preferably it should hold that $t < n$ (Hint: consider a (n, n) secret sharing scheme).

Assume $L = 5$ and consider a $(3, 6)$ secret sharing scheme. Two shares are $(1, 10)$ and $(2, 19)$.

e) (2 pt) Give the polynomial according to which the shares are determined.

f) (1 pt) Give a third share.