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

SECURITY AND CRYPTOGRAPHY (IN4191)

Exam, 14:00-17:00, April 17, 2014

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 Diffie-Hellman (10 pt)

Within a network a Diffie-Hellmann cryptosystem is used. On the basis of a public prime p and a number 'a' and on the basis of a secret X and a public Y a key K is computed that is used for the encryption of the communication between the network. Let the secret key of Alice and Bob be denoted by X(A) and X(B), respectively. The public keys are Y(A) and Y(B). K(A,B) is the key for the encryption of messages between Alice and Bob.

a. (2pt) Give two advantages of key distribution in large networks by means of the Diffie-Hellmann system.
b. (1pt) Describe how an intruder Charles can pose himself as Bob in a communication with Alice.
c. (1pt) Give and explain a method by means of which the authenticity of Alice's public key can be guaranteed on behalf of Bob.
d. (3pt) Assume p=11, a=2, X(A)=9 and X(B)=4. Compute Y(A), Y(B) and K(A,B).
e. (1pt) Assume now that K(A,B) is used for the generation of an AES-key of 128 bits. How large prime p should be at least? Elucidate your answer.
f. (2pt) A third party likes to have retrospectively the possibility to obtain the secret key K(A,B) (fair crypto). Explain how this can be done.

New separate sheet of paper!

Question 2 Shift Registers (10 pt)

a. (2pt) Draw the linear feedback shift register that has 3 registers for the function $f=x_0+x_2$.
b. (2pt) Assuming initial state is 101, generate the first 10 bits using the LFSR in (a).
c. (2pt) Given a random sequence of 1001011, show whether this number satisfies Golomb's 3 criteria or not.
d. (2pt) Assume that a binary file of size 16KB is to be encrypted by XOR'ing with a pseudo random number for **perfect secrecy**. Compute the minimum number of registers needed to generate the pseudo random number using a LFSR. (1 KB is 1024x8 bits).

e. (2pt) Compute the number of different LFSR that can be designed using 4 registers.

New separate sheet of paper!

Question 3 Zero-Knowledge (10 pt)

Alice wishes to prove Bob that she really is Alice. They use the zero-knowledge technique of Fiat & Shamir (as in the course-book). In the initialization phase an independent third party generates for Alice a large number n, which is the product of two large primes p and q. The value of n is public. It also generates for Alice an integer v which is a function of Alice's personal data and computes the value of secret s such that $s^2v=1 \pmod n$.

The protocol itself consists of four steps: 1) Alice sends a value x to Bob which is a function of a random number r selected by Alice. 2) Bob sends a binary value t to Alice. 3) Alice sends to Bob a value y which is based on the value of t among others and which y Bob needs for the verification step. 4) Bob performs the verification step.

a. (3pt) Describe precisely, but only in terms of formulas, how the four steps of zero-knowledge protocol pass after the initialization phase. Herewith assume that Alice selects just one random number r and that Bob performs just one check in order to verify the identity of Alice.

In the following it is assumed that $p=5$, $q=7$, $r=10$ and $s=16$.

b. (2pt) Compute the value of v by means of the Euclidean algorithm(!).
c. (2pt) Compute the values of y if it holds that $t=0$ and $t=1$, respectively.
d. (1pt) Perform the computations that Bob should do for verification in the case of $t=1$
e. (2pt) Assume that in the same session $r=10$ has been used twice by Alice and that Bob sends $t=0$ and $t=1$, respectively. Explain how this can help an intruder like Charles?

New separate sheet of paper!

Question 4 Privacy Preserving Processing (10 pt)

Assume that there are two vectors $X=\{x_1,x_2,\ldots,x_n\}$ and $Y=\{y_1,y_2,\ldots,y_n\}$. Alice has the private key of the additively homomorphic Paillier encryption scheme (that is she has g, n, p and q) and Bob has the public key of Alice (that is g and n).

a. (2pt) Alice has X and Bob has Y. Alice sends her vector in the encrypted form (each term of the vector is encrypted separately). Show that how Bob computes the inner product of X and Y, that is $XY=x_1y_1+x_2y_2+,\ldots,x_ny_n$, using the encrypted vector from Alice.
b. (3pt) Bob has encrypted X and Y and wants to obtain encrypted XY. Bob cannot send the vectors X or Y to Alice as they should be kept secret from her. Write down the secure multiplication protocol for Bob to obtain encrypted XY. Give the number of encryptions, decryptions and exponentiation for your protocol. (Hint: inputs can be masked using random values.)
c. (2pt) Explain using an example why it is important to use fresh random numbers for each encryption of X and Y terms.
d. (3pt) Assuming Alice and Bob each have a single secret bit, explain **briefly** how Bob computes the XOR of these two bits using the garbled circuit approach. (Show the necessary tables and draw the communication between Alice and Bob)