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

CRYPTOGRAPHY (IN4191)

Exam, October 28, 2015
09:00-12:00

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: Diffie-Hellmann key exchange (10 pts)
Alice and Bob want to establish a common secret key K over an insecure channel by using the Diffie-Hellmann key exchange protocol. The private key of Alice is 6 and that of Bob is 15. The primitive element is a= 5 and the computations are performed modulo p, whereby p=23.

a) Compute the public keys of Alice and Bob, as well as their common secret key K. (2 pts)
b) Discuss whether p and a should be kept secret or not? Discuss whether in practice primitive element 'a' should be a small or a large integer? (2 pts)
c) Let K, computed in a), be a shift cipher key (e.g. a Caesar substitution) decipher then the message: EQPITCVWNCVKQPU. (1 pt)
d) Explain in a few sentences, why in general it is difficult for an intruder to find the secret key K (1 pts)
e) In practice the authenticity of the public keys can be a problem. Describe a method by which this can be guaranteed by using Elliptic Curves. (2 pts)

Assume now that that a= 5 and p is p=47, and the public keys of Alice and Bob are 38 and 3, respectively. Which would be as an intruder your strategy for finding the shared secret key K? Elucidate your answer. (2 pts)

Question 2: Modes of DES, perfect secrecy (10 pts)
During the course attention was paid to the so-called'Modes of Des'; ECB, CBC, k-bit CFB and k-bit OFB-mode.

a) Considering these modes can they still be used, if in the corresponding schemes DES is replaced by AES? Elucidate your answer. (1 pt)
b) Draw the scheme of the CBC-mode for encryption. (1pt)
c) If during transmission in the CBC-mode the ciphertext blocks 2, 4 and 7 are changed by the occurrence of errors. Which block will be decrypted incorrectly at the receiver? Give a short explanation. (2 pts)
d) Discuss the advantages and disadvantages if in the CBC-mode DES would be replaced by 3DES. (2 pts)
e) Give the scheme of the k-bit output feedback mode (OFB) (k=64). (1 pt)
f) Explain what 'perfect secrecy' is in the sense of Shannon's theory by using the entropy-concept. (2 pts)

Show that OFB (k-bit OFB (k=64) can lead to a 'perfect secrecy' cipher. (2 pts)

Question 3: RSA (10 points)
Assume that for secure communication, RSA is used. For the key generation, two primes are chosen: p = 7 and q = 13. Answer the following questions based on this information.

a) [3pt] Public key is chosen as e=5. Compute the private key d using the Euclidean algorithm. Give intermediate steps.

b) [2pt] Give the encryption and decryption functions. Explain why it is difficult for an attacker to decipher a ciphertext when only e and n are known.

c) [2pt] Assume that the private key is d=27. Compute the decryption of ciphertext c=8 using the square and multiply approach.

d) [3pt] Assume that Alice wants to encrypt a pdf file of size 10KB. She considers encrypting this document using RSA as she is concerned about the security. For this reason, she uses RSA with a key size of 2048 bits. [1KB=1024x8 bits]

   a. Compute the number of RSA encryptions needed to encrypt this document.
   b. Give 2 reasons to convince Alice that encrypting this file using RSA is not a good idea. **Explain** each reason briefly.
   c. Suggest a better method to send this document to Bob. Note that Alice and Bob do not share a common key.

Question 4: Multi-party Computation (10 points)

a) [2pt] Explain additive homomorphism briefly.
b) [1pt] Explain what kind of homomorphism RSA has.
c) [3pt] Given two encrypted values, namely E(a) and E(b), compute E(10+3a-4b) using additive homomorphism.

d) [2pt] Assume that Alice has an encrypted value, E(m) where m is a 10 bit number, and Bob has the decryption key. Alice sends E(m+r) to Bob where **r** is a random value of size 20 bits. Compute the probability that Bob learns **m** when he decrypts and sees the value m+r. **Hint:** You need to consider the extreme cases.

e) [2pt] Alice creates a garbled circuit to compute **a AND b=c**, where a,b and c are single bits. Alice has **a** and Bob has **b**. Give the number of operations performed in total by Alice and Bob. More precisely, number of AES encryptions, AES decryptions, OT protocol initiated (no need to count the operations within a single OT protocol), and number of (random) keys generated for the garbled circuit construction.