IN4191 Security and Cryptography October 31, 2019

Student Name: ____

Student Number: ____

- The exam consists of 11 pages and 10 questions.
- **Write down your name on each sheet!**
- Answer the questions in the spaces provided on the question sheets. If you run out of room for an answer, continue on the back of the page.
- The teachers need to understand how you got to your answers. Make sure that you take this into account by motivating and explaining your answers. Thus, just stating the final result of your answer without motivation/explanation qualifies for 0 (zero) point.
- During the exam, you may use a simple calculator. Programmable and graphic calculators, laptops, cell phones, books and other materials are not permitted.
- This is a closed-book exam.

Question	**Points**
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
Total	

Student Name: ______________________________

Student Number: ______________________________

1. **Information Theory**

(a) *(3 points)* Use the table to compute $Pr(\mathbb{M} = c | \mathbb{C} = 2)$

$$\mathbb{M} = \{a, b, c, d\} \;;\;\; \mathbb{K} = \{k_1, k_2, k_3, k_4\} \;;\;\; \mathbb{C} = \{1, 2, 3, 4\}$$

$$pr(\cdot) = \{a = \frac{3}{10}, b = \frac{1}{4}, c = \frac{1}{5}, d = \frac{1}{4}\}$$

$$pr(\cdot) = \{k_1 = \frac{1}{4}, k_2 = \frac{1}{4}, k_3 = \frac{1}{4}, k_4 = \frac{1}{4}\}$$

Table 1: Cipher Scheme

	a	b	c	d
k_1	4	1	3	2
k_2	1	3	2	4
k_3	2	4	1	3
k_4	4	2	1	3

(b) *(2 points)* Explain perfect secrecy briefly. What is the condition for an encryption scheme to be perfectly secure?

Student Name: ____

Student Number: _______________________________________

2. **Defining Security**

   (a) *(1 point)* What is IND-CPA security?

   (b) *(1 point)* What is IND-CCA security?

   (c) *(3 points)* Analyse the security of El Gamal encryption scheme. Show whether it is IND-CPA and/or IND-CCA secure.

Student Name: ____

Student Number: ______________________________________

3. **Block Ciphers**

   (a) *(2 points)* Describe the Shannon's diffusion-confusion paradigm briefly (No more than 25 words for each property).

   (b) *(1 point)* State the role of matrix multiplication operation (mixColumn) in AES regarding the diffusion-confusion properties.

   (c) *(2 points)* In DES block cipher, each S-Box is 6×4-bit and it is not invertible. However, AES uses an 8×8-bit invertible S-box. Explain (both) why it is necessary to have invertible S-boxes in AES, whereas not in DES.

Student Name: ______________________________
Student Number: ______________________________

4. **Modes of Operation**

Let a message $M = m_1 \| m_2 \| m_3 \| m_4$ be encrypted with AES by using one of the modes of operations (m_i is 128-bit). Corresponding ciphertext is $C = c_1 \| c_2 \| c_3 \| c_4$. C is transmitted in a noisy channel and one of the following occurs:

1. The second bit of c_2 is flipped.
2. The order of c_2 and c_3 is changed, i.e., $C' = c_1 \| c_3 \| c_2 \| c_4$.
3. c_2 is dropped, i.e., it is not received by the receiver part.

Receiver obtains plaintext $M' = m'_1 \| m'_2 \| m'_3 \| m'_4$ (or $M' = m'_1 \| m'_2 \| m'_3$ for the last case) by decrypting the received ciphertext. Note that the receiver is not aware of the losses caused by the noisy channel. **Consider CBC and CTR modes**.

(a) *(3 points)* Analyse the difference between M and M' for each noisy channel (with each modes of operations).

(b) *(2 points)* For each noisy channel, find the best modes of operation algorithm(s) among CBC and CTR modes. In other words, find the one(s) with the minimum message lost.

Student Name: ______________________________

Student Number: ______________________________

5. **Hash Functions**

Show that the following hash functions are not secure (for at least one of security properties collision, preimage or second preimage attacks).

(a) *(3 points)*

$$H_1(m_1||m_2) = E_{m_1}(m_1) \oplus m_2 \tag{1}$$

where the hash function takes 256-bit input message $m_1||m_2$ and uses the first 128-bits both as the key and the message for the $E_k(m)$ encryption algorithm, XORs the result with the rest of the message, and outputs a 128-bit hash. Here, $E_k(m)$ is a secure encryption algorithm with 128-bit key length and 128-bit block size.

(b) *(2 points)*

$$H_2(m) = m^e \bmod N \tag{2}$$

where the hash function takes 256-bit input message m and generates the ciphertext of RSA encryption algorithm as the hash output. Here, $N = p \times q$ is 2048-bit RSA modulo and e is co-prime with $\phi(N)$ and assume that e, p and q are publicly known.

Student Name: ____________________

Student Number: ____________________

6. **RSA**

A (textbook) RSA encryption scheme is set up with public key $N = 551 = 19 \times 29$ and $e = 275$.

(a) *(2 points)* Find the private key d via Extended Euclidean Algorithm.

(b) *(1 point)* Provide the decryption function and decrypt the ciphertext $c = 4$.

(c) *(2 points)* For the same RSA encryption scheme $N = 551$ and $e = 275$, assume that it is not feasible to factorize N and you do not have the private key d.

You are given two plaintext and ciphertext pairs generated with this encryption algorithm: $(m_1, c_1) = (276, 3)$, $(m_2, c_2) = (473, 6)$.

Can you still decrypt the ciphertext $c = 4$? If yes, show each step of your decryption. Otherwise, explain why it is not possible.

Student Name: ____

Student Number: ____

7. **Public Key Encryption**

El Gamal encryption scheme can be defined in the following three steps: Key Generation, Encryption, Decryption.

KeyGen: $\mathbb{G}$ is cyclic group of order p, with generator g.
$sk: \ x \leftarrow \mathbb{Z}_p$,
$pk: \ (h \leftarrow g^x \bmod p \ , \mathbb{G}, p, g)$

Enc: For a message $m \in \mathbb{G}$
$r \leftarrow \mathbb{Z}_p$
$c_1 \leftarrow g^r \ , c_2 \leftarrow m \cdot h^r$,
Ciphertext := $(c_1 \ , c_2)$.

Dec: $m := c_2 \cdot c_1^{-x} \bmod p$

(a) *(2 points)* Show the homomorphic property of El Gamal encryption scheme. Is it additively or multiplicatively homomorphic? Explain whether this property is related to IND-CPA security or IND-CCA security.

(b) *(3 points)* Apply Fujisaki-Okamoto transformation on El Gamal encryption scheme. What is the effect of the transformation on the security?

Student Name: ______________________________

Student Number: ______________________________

8. **Public Key Systems**

   (a) *(3 points)* Explain Fujisaki-Okamoto Transformation. What is the purpose of this transform and show how it can be applied to the RSA scheme?

   (b) *(2 points)* Explain Key Encapsulation Mechanism (KEM) and its use.

Student Name: ____

Student Number: ______________________________________

9. **Key Agreement**

   (a) *(2 points)* Imagine that there are 2 ways of computing the hash of two values: 1) $H(a||b)$ and 2) $H(a, b)$ where || denotes the string concatenation. Explain the difference, also in terms of security.

   (b) *(1 point)* Explain the reasons of using nonce in key establishment protocols in general.

   (c) *(2 points)* Explain why Signed Diffie-Hellman key exchange protocol is not secure.

Student Name: ______________________________

Student Number: ______________________________

10. **Secret Sharing**

   (a) *(1 point)* Consider the polynomial $y = x^3 + 2x^2 + 6$ in $\mathbb{Z}_{11}$. Calculate the points where $x = 1$, $x = 2$, $x = 3$, $x = 4$ and $x = 5$.

   (b) *(1 point)* For the same polynomial, what is the minimum number of points needed to reconstruct the polynomial? Justify your answer.

   (c) *(3 points)* For a second degree polynomial passing through $(1, 0)$, $(2, 1)$ and $(3, 2)$ in $\mathbb{Z}_5$, reconstruct the polynomial using Lagrange Interpolation. What is the secret value?