Student Name: _____
Student Number: _____

- The exam consists of 13 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 $Pr(\mathbb{M} = c|\mathbb{C} = 2)$

$$\mathbb{M} = \{a, b, c, d\} \; ; \quad \mathbb{K} = \{k_1, k_2, k_3, k_4\} \; ; \quad \mathbb{C} = \{1, 2, 3, 4\}$$
$$pr(\cdot) = \{a = \frac{3}{10}, b = \frac{1}{4}, c = \frac{1}{5}, d = \frac{1}{4}\}$$
$$pr(\cdot) = \{k_1 = \frac{1}{4}, k_2 = \frac{1}{4}, k_3 = \frac{1}{4}, k_4 = \frac{1}{4}\}$$

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

Solution:

$$p(\mathbb{M} = c|\mathbb{C} = 2) = \frac{p(\mathbb{C} = 2|\mathbb{M} = c) \cdot p(\mathbb{M} = c)}{p(\mathbb{C} = 2)} \; .$$

$p(\mathbb{C} = 2) = \frac{3}{10} \cdot \frac{1}{4} + \frac{1}{4} \cdot \frac{1}{4} + \frac{1}{5} \cdot \frac{1}{4} + \frac{1}{4} \cdot \frac{1}{4} = \frac{1}{4}$.

$p(\mathbb{C} = 2|\mathbb{M} = c) = \sum_{k:c=d_k(2)} p(\mathbb{K} = k) = \frac{1}{4}$.

$p(\mathbb{M} = c) = \frac{1}{5}$.

$p(\mathbb{M} = c|\mathbb{C} = 1) = \frac{\frac{1}{4} \cdot \frac{1}{5}}{\frac{1}{4}} = \frac{1}{4}$.

(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.

Solution:

- provide the explanation based on the text book: chosen plaintext attack where the attacker has encryption oracle in addition to LR-oracle.
- provide the explanation based on the text book: chosen ciphertext attack where the attacker has decryption oracle in addition to LR-oracle and encryption oracles.
- Considering the encryption function, El-Gamal is probabilistic and homomorphic. (Here mathematical explanation is required). Thus, it is IND-CPA secure and not IND-CCA secure. [A proof about CCA security is required here.]

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).

Solution: Confusion: Introducing non-linearity and making the relation between input and output as complex as possible.

Diffusion: Diffusing the bit effects to the whole block.

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

Solution: Matrix multiplication is a linear operation where the 4 byte state is multiplied with 4×4 byte matrix. This multiplication diffuses the bit changes in a byte to the others. It is the main source for the diffusion property.

(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.

Solution: Each block cipher needs to be reversible to in order to obtain the plaintext from the ciphertext.

DES has a Feistel structure and the Feistel function does not have to be invertible to reverse the round operation.

On the other hand, AES has SPN structure. For that reason, each operation in SPN structure should be reversible including S-Boxes.

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.

Solution: In CBC mode, every ciphertext block is used to feed the next plaintext block. This would cause spread of the errors in the following blocks. In this manner,

- m_2 and m'_2 will be totally different because of the avalanche effect in AES. Also, the second bit of m'_3 will be different than m_3 because of the feedback. The rest will be the same.
- Only the first block will be recovered. The rest will be unrelated with the original blocks because of the change in decryption and feedback orders.
- Similar to the previous case, the first block will be recovered. The last block will be recovered as third block since it is depending on c_3 and c_4, i.e., $m'_3 = m_4$

In CTR mode, blocks are also independent. In addition, the ciphertext blocks do not interact with the AES directly, instead counter value does. In this manner,

- The second bit of m'_2 will be different than m_2. The rest will be the same. $M' = m_1||m_2^{b2}||m_3||m_4$.
- Change in orders causes change in counter values of the blocks. Because of the avalanche effect of the AES, one bit change in counter values will result in totally different blocks. Therefore, m'_2 and m'_3 will be totally

unrelated with the original plaintext blocks. First and the last blocks will be recovered correctly. $M' = m_1||r||r||m_4$.

- Since he is not aware of the drop, he cannot recover other than the first block. The rest will be unrelated with the original message. This is because one more increment in counter value will result in a totally different value. $M' = m_1||r||r$.

Therefore, the best performing MoOs for each channel can be found as:

- CTR: only one bit loss, whereas CBC lose a block and a bit of next block
- CTR: two blocks are recovered
- CBC: two blocks are recovered

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.

Solution:

For H_1 hash function, an adversary can easily find a second preimage of a message. Second preimage attack is finding second message which has the same digest with the chosen message. Let $M = m_1||m_2$ is given to the adversary, and h is the digest of the message. Adversary can use message n_1 (different from m_1) and compute $E_{n_1}(n_1)$ and obtain $n_2 = h \oplus E_{n_1}(n_1)$. Because of the hash construction $H(n_1||n_2) = H(m_1||m_2) = h$, meaning that $N = n_1||n_2$ is another message having the same digest value h. Therefore, the hash function is not second preimage resistant.

For H_2 hash function, an adversary can easily find a preimage of a hash. Preimage attack is finding a message m for a given hash h such that $H_2(m) = h$. In H_2 hash function, it can be seen that the hashing operation is the same with RSA encryption. Since, p and q are known primes, by using extended Euclidean algorithm, the private key d of the RSA can be computed such that $e \cdot d \equiv 1 \bmod (p-1)(q-1)$. For any given hash value $h = H_2(m)$, the preimage can be computed with the following formula: $h^d \bmod N$. Thus, H_2 is not preimage resistant.

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.

Solution:

$$d \equiv e^{-1} \bmod \phi(N), \quad e = 275,\ \phi(N) = 18 \cdot 28 = 504$$

By using extended Euclidean Algorithm

$$504 = 275 * 1 + 229,\ 275 = 229 * 1 + 46 \implies 229 = 46 * 4 + 45$$
$$46 = 45 * 1 + 1 \implies 1 = 46 - 45 = 46 - (229 - 46 * 4) = 46 * 5 - 229$$
$$= (275 - 229) * 5 - 229 = 275 * 5 - 229 * 6 = 275 * 5 - (504 - 275) * 6$$
$$= 275 * 11 - 504 * 6 \implies 275 * 11 \equiv 1 \bmod 504 \implies d = 11.$$

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

Solution:

$$m \equiv c^d \bmod N \implies m \equiv 4^{11} \bmod 551 \implies m = 92.$$

(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.

Solution: Using the homomorphic properties of RSA, we can find the decryption of 4 as follows:

$$m = c^d \bmod N = 4^d \bmod 551 = ((\frac{c_2}{c_1})^2)^d \bmod 551$$
$$m = ((\frac{c_2}{c_1})^2)^d = (\frac{m_2}{m_1})^2 \bmod 551 = 473^2 \cdot (276^{-1})^2 \bmod 551.$$

Inverse of 276 in modulo 551 can be found by Extended Euclidean Algorithm:

$$551 = 276 \cdot 1 + 275 \quad 276 = 275 \cdot 1 + 1$$
$$\implies 1 = 276 - 275 = 276 - (551 - 276) = 2 \cdot 276 - 551.$$

Then, the message can be computed as follows:

$$m = 473^2 \cdot (276^{-1})^2 \bmod 551 = 23 \cdot 2^2 \bmod 551 = 92.$$

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.

Solution:
(0.5 points) El Gamal encryption scheme is multiplicatively homomorphic.

(0.5 points) In other words, it is malleable. For that reason, it cannot be IND-CCA secure.
(1 point) Let ciphertext of message m would be c_1, c_2 and similarly for m' the ciphertext would be c_1', c_2'.
The ciphertext of $M = m \cdot m'$ can be computed as $C_1 = c_1 \cdot c_1'$ and $C_2 = c_2 \cdot c_2'$

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

Solution: (2 points) Let H be the secure hash function. Then, El Gamal encryption algorithm transforms into:

$$Enc'(m, r) = Enc(m\|r, H(m\|r)) = (g^{H(m\|r)}, (m\|r) \cdot h^{H(m\|r)}) \tag{3}$$

(1 point) The effect is that Fujisaki-Okamoto transformation enhances the security of the encryption algorithm from IND-CPA to IND-CCA.

Student Name: _____
Student Number: _____

8. **Public Key Systems**

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

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

Solution:

- Fujisaki-Okamoto transform is as follows: $E(m, r) \rightarrow E(m||r, H(m||r))$ to make an IND-CPA secure scheme IND-CCA secure. It cannot be applied to RSA as it is not IND-CPA secure. (a correct mapping from m to m||r will be accepted).
- KEM relies on a secure algorithm that outputs a session key which is encrypted with the public key of the recipient. Using the ciphertext and the secret key, the recipient can reproduce the session key and decrypt the message. [a figure here is needed.]

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.

Solution:

- $H(a||b)$ is open to collusions: $H(a||aabb) = H(aa||abb)$. Thus, it is not secure. However, $H(a, b)$ clearly indicates that hash function is based on 2 data inputs a and b. Depending on the implementation, it is secure.
- Signed version is still not secure since Eve can change the signatures easily. This is because the signatures are not linked to the identities. [more explanation is needed here.]

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 $x = 5$.

Solution: $(1, 9), (2, 0), (3, 7), (4, 3), (5, 5)$

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

Solution: $t - 1 = 3$ then $t = 4$.

(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?

Solution: $y = x^2 + 3x + 1$ and $s = 1$.
There is a typo in the question. Thus, the solutions seems to be a line: $y = x - 1$. Anyone who found that got full points.