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. Scientific and graphic calculators, laptops, cell phones, books and other materials are not permitted.
- This is a closed-book exam.

Student Name: _____
Student Number: _____

1. **Stream Ciphers**

(a) *(5 points)* b_i is a bit sequence with period P and it is given that $b_i = b_{i+K}$ for all i's. Show that P divides K.

Student Name: _____

Student Number: _____

2. **Block Ciphers**

(a) *(5 points)* Explain properties of the Feistel structure used in DES.

Student Name: _____
Student Number: _____

3. **Modes of Operations**

(a) *(5 points)* Let a message $M = m_1\|m_2\|m_3\|m_4$ be encrypted with AES by using the CFB (ciphertext feedback) mode (m_i is 128-bit), and 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

- The second bit of c_2 is flipped.
- The order of c_2 and c_3 is changed, i.e., $C' = c_1\|c_3\|c_2\|c_4$.
- c_2 is dropped, i.e., it is not received by the receiver part (receiver is not aware of the drop).
- c_2 is dropped, i.e., it is not received by the receiver part (receiver is aware that the second block is dropped).

Receiver obtains plaintext $M' = m'_1\|m'_2\|m'_3\|m'_4$ (or $M' = m'_1\|m'_2\|m'_3$ for the last two cases) by decrypting the received ciphertext. Examine the difference between M and M' for each case.

CFB Mode:

$$C_0 = IV$$
$$C_i = E_K(C_{i-1}) \bigoplus P_i$$

Note: Show the relations in a formal way, use m^{b2} to represent second bit flipped version of m, and r to represent a random (or totally distorted) block. An example would be $m'_1 = m_2, m'_2 = r, m'_3 = m_4^{b2}$ (for one of the last 2 cases).

Student Name: _____

Student Number: _____

4. **RSA**

(a) *(10 points)* Let $sk = (d, p, q)$ be the secret key of a basic RSA signature scheme. Suppose $d_p = d \pmod{p-1}$ and $d_q = d \pmod{q-1}$. Assume both p and q have bit-length $l_p = l_q = k$ and that d has bit-length $l_d = 2k$. Assume the square-and-multiply algorithm takes time $1.5 \cdot l_d \cdot (l_n)^2$ (with $l_n = l_p + l_q$) to compute $\sigma = m^d \pmod{n}$ for message $m \in \mathbb{Z}_n$. Compare the time necessary to compute σ with and without using the Chinese Remainder Theorem (CRT). You may assume when using the CRT that the time to combine the partial solutions ($\sigma_p = \sigma \pmod{p}$ and $\sigma_q = \sigma \pmod{q}$) is negligible and can be ignored.

Student Name: _____

Student Number: _____

5. **PRFs**

(a) *(5 points)* A pseudorandom function $F : \{0,1\}^n \times \{0,1\}^m \rightarrow \{0,1\}^\ell$ is an efficiently computable function that given a key k and an input x computes an output $y = F_k(x)$. Informally, F is a pseudorandom function if $F_k(\cdot)$ looks like a random function. Formally, we define F to be (t, ϵ) - secure if for all t-bounded adversaries Adv we have:

$$|Pr[k \leftarrow \{0,1\}^n : Adv^{F_k(\cdot)}(1^n) = 1] - Pr[R \leftarrow RandomFunc(m, \ell) : Adv^{R(\cdot)(1^n)} = 1]| \leq \epsilon$$

Name a well-known and standardized function $F : \{0,1\}^{256} \times \{0,1\}^{128} \rightarrow \{0,1\}^{128}$ that is believed to be a *pseudorandom permutation.* Explain your answer.

Student Name: _____

Student Number: _____

6. **ElGamal Encryption**

(a) *(5 points)* The scheme $\Pi = (KeyGen, Enc, Dec)$ represents the ElGamal cryptosystem. Provide the algorithms for the scheme (i.e the algorithms for each of $KeyGen, Enc$ and Dec).

Student Name: _____

Student Number: _____

7. **Diffie-Hellman**

(a) *(5 points)* Explain the Decisional Diffie-Hellman, Discrete log and Computational Diffie-Hellman assumptions and show their relationship.

Student Name: _____
Student Number: _____

8. **Hash Functions**

(a) *(5 points)* Define collision resistance property of a cryptographic hash function. Provide the expected bit security of a cryptographic hash function, having 128-bit digest size, regarding collision attack.

Student Name: _____

Student Number: _____

9. **Key Exchange**

(a) *(5 points)* Alice and Bob would like to create a shared key using the Elliptic Curve version of the Diffie-Hellman key exchange protocol. Provide the domain parameters and the protocol.

Student Name: _____

Student Number: _____

10. **Secret Sharing**

Given the polynomial $P(x) = 3x^2 + 6x + 7 \bmod 11$, five parties, A, B, C, D and E, would like to participate in a (t, n)-threshold secret sharing scheme. The following set of users can obtain the secret:

1. A and B
2. B and C
3. A, C and D
4. D, C, and E.

(a) *(1 point)* What is the secret?

(b) *(1 point)* What is the minimum value of t?

(c) *(3 points)* Determine the number of shares for each party and produce those shares: $s_1, s_2, s_3, \ldots, s_n$.