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.

Solution: By definition of period, P is the smallest integer such that $b_i = b_{i+P}$ for all (sufficiently large) i. Then, $K \geq P$.
Let assume P does not divide K, and remainder of K in modulo P is R, i.e., $K = P \cdot A + R$ for $A \geq 1$ and $P > R \geq 0$.

$$b_i = b_{i+K} = b_{i+K-A \cdot P} \quad \text{(by definition of period)}$$
$$\implies b_i = b_{i+R} \quad \text{(for all (sufficiently large) } i\text{)}$$

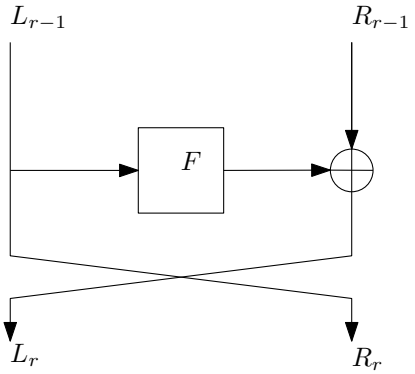
which contradicts with P being the smallest value. Therefore, R must be equal to zero, in other words, K should be multiple of P.

Student Name: _____
Student Number: _____

2. **Block Ciphers**

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

Solution:



As illustrated above, Feistel structure round function works as

Encryption	Decryption
$R_r = L_{r-1}$	$L_{r-1} = R_r$
$L_r = F(L_{r-1}) \oplus R_{r-1}$	$R_{r-1} = L_r \oplus F(R_r)$

It can be seen that both encryption and decryption operations require only F, not inverse of it. Therefore,

- F does not have to be invertible,
- It is hardware-efficient because the encryption function can be also used for the decryption (with reversed ordered round keys).

Second property is that only half of the block is encrypted which results in

- Smaller hardware and faster software because half of data is not processed,
- Late diffusion of the key and non-linear operations.

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).

Solution: Let us investigate each case with the same order given in question;

- Bit flip in c_2 yields one bit difference in second block and totally disturbed third block (because of the encryption). It will not affect first and last blocks. Therefore, $M' = m_1||m_2^{b2}||r||m_4$.
- The order change affects the last three blocks since they all xored with misplaced values. The first block is not affected since it is involved with IV and c_1. The result will be $M' = m_1||r||r||r$.
- If c_2 is dropped, then second and third blocks cannot be recovered. Since the first and last blocks do not depend on c_2, they will be decrypted correctly. The output will be $M' = m_1||r||m_4$.
- The result will be the same regardless of the awareness of the receiver. Thus, $M' = m_1||r||m_4$.

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.

Solution: Using the Chinese Remainder Theorem we get:

$$\begin{aligned}
\sigma_p &= m^d \mod p = m^{d \bmod p-1} \mod p \\
&= m^{d_p} \mod p = (m \mod p)^{d_p} \mod p = (m_p)^{d_p} \mod p \\
\sigma_q &= m^d \mod q = m^{d \bmod q-1} \mod q \\
&= m^{d_q} \mod q = (m \mod q)^{d_q} \mod q = (m_q)^{d_q} \mod q \,.
\end{aligned}$$

Therefore, when computing $\sigma_p = (m_p)^{d_p} \mod p$ and $\sigma_q = (m_q)^{d_p} \mod q$, the values m_p, m_q, d_p and d_p have $k - bits$. Hence, computing σ takes time $t = 2 \cdot (1.5 \cdot (k)^2 \cdot k) = 3k^3$.
However, without the CRT, this computation will take time $t' = 1.5 \cdot (2k)^2 \cdot 2k = 12k^3 = 4t$.

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.

Solution: AES, with 256-bit keys.
The function $F : \{0,1\}^{256} \times \{0,1\}^{128} \rightarrow \{0,1\}^{128}$ represents
256-bit key $\times$ 128-bit block input $\rightarrow$ 128-bit block output.
The 128-bit block output appears random and an adversary cannot efficiently distinguished the output from a random 128-bit string, and also cannot efficiently invert the output without the knowledge of the 256-bit key stream.

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).

Solution:
$\Pi = (keyGen,\ Enc,\ Dec)$
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: $m := c_2 \cdot c_1^{-x} \bmod p$

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.

Solution:
Discrete Log: In a cyclic group $\mathbb{G}$ of order p with generator g. Where p is large. Given g^a, g, where $a \leftarrow \mathbb{Z}_p$, it is hard to efficiently compute a from g^a.
CDH: $a, b \leftarrow \mathbb{Z}_p$, Given $(g\ , g^a\ , g^b)$ it is hard to efficiently compute g^{ab} .
DDH: $a, b, c \leftarrow \mathbb{Z}_p$, Given $(g\ , g^a\ , g^b)$ it is hard to efficiently distinguish g^{ab} from g^c .

If **DDH** is hard, then **CDH** must be hard. And if **CDH** is hard, then **Discrete Log** must be hard.
DDH is a weaker assumption than **CDH** and **CDH** is a weaker assumption than **Discrete Log**.

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.

Solution: Collision in a hash function refers to two different messages m_1 and m_2 having the same digest $H(m_1) = H(m_2)$. Since hash functions have arbitrary input size and fixed digest size, it is obvious that there will be infinitely many collisions for any hash function (unless the domain is constrained).

A cryptographic hash function is counted secure against collision attack if it is not feasible to find a collision. Formally, finding collision complexity should not be lower than the birthday bound. Birthday bound is approximately equal to the square root of the size of the output set. In our case, hash function having 128-bit digest should provide 64-bit security against collision attacks.

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.

Solution: Given the elliptic curve E, choose a point G on E which has a prime order $q = \#E(\mathbb{F}_q)$ where p is a prime number.

1. Alice generates random integer $a \in \{1, \ldots, q-1\}$ and computes aG, and sends it to Bob.
2. Bob generates random integer $b \in \{1, \ldots, q-1\}$ and computes bG, and sends it to Alice.
3. Alice computes the shared key $K = a(bG) = abG$
4. Bob computes the shared key $K = b(aG) = abG$.

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?

> **Solution:** The secret value is the constant of the polynomial, that is 7.

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

> **Solution:** Given the polynomial of degree $t - 1 = 2$, $t = 3$ shares are needed to reconstruct the polynomial and obtain the secret.

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

> **Solution:** Given the combination, the number of shares for each party should be as follows: A, C, D, and E should have 1 share each, and B should have 2 shares. Then, A is given $s_1 = (1, P(1))$, B is given $s_2 = (2, P(2))$ and $s_3 = (3, P(3))$, C is given $s_4 = (4, P(4))$, D is given $s_5 = (5, P(5))$ and E is given $s_6 = (6, P(6))$. Then the shares are as follows: $s_1 = (1, 5)$, $s_2 = (2, 9)$, $s_3 = (3, 8)$, $s_4 = (4, 2)$, $s_5 = (5, 10)$ and $s_6 = (6, 8)$.