Full name: _____

Student ID: _____

- This exam is made of 11 pages and **10 questions**.
- You work individually on your answers. With the submission of your answers, you declare that this is your **individual work** and you did not ask any other person for assistance. You neither discussed with fellow students nor asked in an internet forum or chat for help.
- Explain and **motivate** all your answers.
- You have **180 minutes** to do the exam (+45 if you are entitled for extra time).
- Make sure your **handwriting is clear** and legible. 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.
- This is a **closed-book** exam.

Exercise 1 – Perfect Security

[10 points] We have a cipher with three messages $\mathcal{M} := \{m_1, m_2, m_3\}$, five keys $\mathcal{K} := \{k_1, k_2, k_3, k_4, k_5\}$, and four possible ciphertexts $\mathcal{C} := \{c_1, c_2, c_3, c_4\}$, defined by the following encryption map:

	k_1	k_2	k_3	k_4	k_5
m_1	c_1	c_3	c_2	c_4	c_4
m_2	c_4	c_4	c_4	c_3	c_1
m_3	c_2	c_1	c_3	c_1	c_4

(a) **[2 points]** Based on the cardinalities of the message, ciphertext and key spaces, can the above cipher be perfectly secret, in principle? Explain why.

(b) **[4 points]** Assuming plaintext and key distributions to be uniform, compute $\Pr[C = c]$ for each ciphertext $c \in \mathcal{C}$.

(c) **[4 points]** Under the same distribution assumptions, determine whether this cipher is perfectly secure, and prove your statement.

Exercise 2 – PRG and PRF [10 points]

(a) **[4 points]** Let G be a PRG with expansion factor ℓ such that $\ell(n) > n$ for all $n \in \mathbb{N}$, and consider this definition for G':

$$G'(s) = G(s)^{\#} \ ,$$

where for all $n \in \mathbb{N}$ and $i \in \{1, \cdots, \ell(n)\}$ we have

$$G(s)^{\#}_i = \begin{cases} 1 & \text{, if } i \equiv 1 \mod 2 \\ G(s)_i & \text{, otherwise} \end{cases}$$

Is G' a PRG? Motivate your answer. It is not necessary to provide a full proof by reduction or a worked out counterexample, but you should at least provide the intuition behind your answer (for example: if you think that G' is not a PRG, then you should describe a strategy for a distinguisher).

(b) **[3 points]** Let $\mathbb{F} = \{f_s\}$ be a pseudorandom function where $f_s : \{0,1\}^{|s|} \to \{0,1\}^{|s|}$, and consider the new function f'_s defined for all $x \in \{0,1\}^*$ as:

$$f'_s(x) = f_s(x_R)$$

where for all $x \in \{0,1\}^*$, x_R is the string x taken in reverse order. Is f'_s a PRF as well? Motivate your answer, again by describing the intuition behind it.

(c) **[3 points]** Provide the formal definition of a strong pseudorandom permutation. What cryptographic primitive is a good candidate of such a permutation?

Exercise 3 – Boolean Functions and Stream Ciphers [10 points]

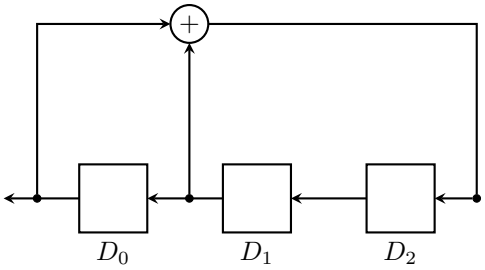
Consider the Boolean function $f : \{0,1\}^3 \to \{0,1\}$ defined for all $(x_1, x_2, x_3) \in \{0,1\}^3$ as:

$$f(x_1, x_2, x_3) = \begin{cases} x_1 & , \text{ if } x_2 = 1 \text{ and } x_3 = 1 \\ x_1 \oplus 1 & , \text{ otherwise} \end{cases}$$

1. [**4 points**] Write the truth table of the function.
2. [**2 points**] Is the function balanced?
3. [**4 points**] Briefly describe the combiner generator model for stream ciphers. Could function f be used in such a model?

Exercise 4 – LFSR [10 points]

Consider the following LFSR:



1. **[6 points]** Is this a maximum-length LFSR? Draw the full transition graph where the nodes represent the states of the registers.
2. **[4 points]** If we start from the initial state $(0, 1, 1)$, what are the first 8 bits generated in output for the keystream? When do they start repeating?

Exercise 5 – Block Ciphers and Mode of Operations [10 points]

(a) [**10 points**] A company is developing their own symmetric cipher. Their website is claiming that the underlying block cipher is based on the substitution-permutation network paradigm. For enhanced security, the block cipher has both a block length and key length of 1024 bits, and it runs for 128 rounds. The confusion layer of this SPN cipher, on the other hand, is defined by S-boxes of the form $F : \{0,1\}^8 \to \{0,1\}^4$, to ensure irreversibility of the ciphertexts. Further, they extend this cipher with CBC mode to encrypt plaintexts of arbitrary length. For efficiency, only the first plaintext is encrypted using a random IV. Then, they use the last ciphertext block as a new IV for the next plaintext to encrypt.

Analyze the security and efficiency issues of the cipher described above.

Exercise 6 – Message Authentication Codes [10 points]

Unconditionally Secure MACs

[6 points] Alice and Bob use a secure MAC $(\mathcal{M}, \mathcal{A}, \mathcal{K}, \mathsf{Gen}, \mathsf{Mac}, \mathsf{Vrfy})$ to authenticate their messages, where $\mathcal{M} = \{0, 1, \cdots, 11\}$, $\mathcal{A} = \mathbb{Z}_{13}$ and $\mathcal{K} = \mathbb{Z}_{13} \times \mathbb{Z}_{13}$. The key generation algorithm Gen simply samples with uniform probability a key from $\mathcal{K}$, while the tag generation algorithm is defined for all keys $k = (i, j) \in \mathcal{K}$ and messages $m \in \mathcal{M}$ as:

$$\mathsf{Mac}_k(m) = (i + mj) \mod 13 \ .$$

Since 13 is prime, we know that the corresponding authentication matrix is an orthogonal array, so the MAC is unconditionally secure.

(a) **[2 points]** Oscar observes the pair $(10, 6)$ on the channel, where the first component is the message while the second is the corresponding authenticator. What is the probability for Oscar to guess the correct key?

(b) **[4 points]** Alice and Bob commit a mistake and use the same key $k = (i, j)$ to authenticate another message after $m = 10$. In particular, after seeing $(10, 6)$, Oscar sees the pair $(7, 4)$. What is the key shared by Alice and Bob? Explain in detail how Oscar can retrieve it, assuming that the tag generation algorithm is public.

Computationally Secure MACs

[4 points] Turn the following informal description of a MAC scheme into a formal description, then prove its insecurity: to authenticate a message, we XOR it with its reverse (i.e. the same message but with the bits in reverse order), and apply a pseudorandom function to the result of the XOR.

Exercise 9 – Hash Functions

[10 points] Let $\mathcal{H} = (\mathsf{Gen}, H)$ be a hash function.

(a) **[3 points]** Provide a formal definition for the collision resistance property, by formulating a security game (similar to the ones defined below for similar properties).

Remember now the following two definitions.

Definition 1 (Preimage Resistance). A hash function $\mathcal{H} = (\mathsf{Gen}, H)$ is preimage resistant if for all PPTA $\mathcal{A}$ there is a negligible function negl such that

$$\Pr[\mathsf{Hash\text{-}preimage}_{\mathcal{A},\mathcal{H}}(n) = 1] \leq \mathsf{negl}(n)$$

where $\mathsf{Hash\text{-}preimage}_{\mathcal{A},\mathcal{H}}(n)$ is the following game:

1. $s \leftarrow \mathsf{Gen}(1^n)$
2. $x \leftarrow \{0,1\}^*$
3. $y := H^s(x)$
4. $x' \leftarrow \mathcal{A}(s, y)$
5. Return 1 if $H^s(x') = y$, 0 otherwise.

Definition 2 (Second Preimage Resistance). A hash function $\mathcal{H} = (\mathsf{Gen}, H)$ is second preimage resistant if for all PPTA $\mathcal{A}$ there is a negligible function negl such that

$$\Pr[\mathsf{Hash\text{-}preimage2}_{\mathcal{A},\mathcal{H}}(n) = 1] \leq \mathsf{negl}(n)$$

where $\mathsf{Hash\text{-}preimage2}_{\mathcal{A},\mathcal{H}}(n)$ is the following game:

1. $s \leftarrow \mathsf{Gen}(1^n)$
2. $x \leftarrow \{0,1\}^*$
3. $x' \leftarrow \mathcal{A}(s, x)$
4. Return 1 if $x' \neq x$ and $H^s(x') = H^s(x)$, 0 otherwise.

(b) **[7 points]** Does one of the two properties defined above imply the other? If yes, which one implies which? Formally prove your statement.

Exercise 8 – Primality Testing and Group Generators [10 points]

(a) **[6 points]** Using the Fermat's primality test, show that the number 29 is composite with a probability less than 20%.

(b) **[4 points]** Consider the multiplicative group $\mathbb{Z}_{29}^*$. What are the possible orders of its subgroups?

Exercise 9 – Diffie-Hellman Key Agreement [10 points]

Alice and Bob want to agree on a common secret key using the Diffie-Hellman Key Agreement protocol.

(a) **[5 points]** They are using the multiplicative group $G = \mathbb{Z}_7^*$ and the generator $g = 2$. Manually execute the DH protocol between Alice and Bob, with secret exponents being respectively $a = 6$ and $b = 2$.

(b) **[5 points]** Explain the correctness of the DH Key Agreement protocol (i.e., show why, in general, Alice and Bob generate the same key).

Exercise 10 – RSA Cryptosystem [10 points]

Alice wants to send a message to Bob using the RSA cryptosystem.

(a) Bob creates an RSA key pair with primes $p = 7$ and $q = 11$, and public exponent $e = 7$. Compute the public and private key pair for Bob.

(b) Alice encrypts the message $m = 6$. Compute the corresponding ciphertext.