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 Secrecy [10 points]

Consider the following cipher with three messages, $\mathcal{M} := \{m_1, m_2, m_3\}$, four keys $\mathcal{K} := \{k_1, k_2, k_3, k_4\}$, and four 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
m_1	c_2	c_1	c_3	c_4
m_2	c_4	c_3	c_1	c_2
m_3	c_1	c_2	c_4	c_3

(a) [**5 points**] Assuming plaintext and key distributions to be uniform, does this cipher satisfy perfect secrecy? Motivate your answer, and show at least one example of calculation of the conditional probabilities $Pr(M = m|C = c)$ in detail.

(b) [**5 points**] Suppose that we *swap* the plaintext space with the key space above, i.e. we now have $\mathcal{M} = \{m_1, m_2, m_3, m_4\}$ and $\mathcal{K} = \{k_1, k_2, k_3\}$. The ciphertext space remains unchanged. The encryption table is instead re-defined as the *transpose* of the encryption table above. Write the new encryption table in full. Does the marginal distribution $Pr(C = c)$ of the ciphertexts change? Is this new cipher perfectly secret? Motivate your answers. As above, you can assume that the new plaintexts and keys are uniformly distributed.

Exercise 2 – PRG and PRF [10 points]

(a) **[3 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 $s \in \{0,1\}^*$ such that $|s| = n$ and $s = s_1 s_2 \cdots s_n$, we have $s^* = s_1^* s_2^* \cdots s_n^*$ where

$$s_i^* = \begin{cases} 0 & \text{, if } i \equiv 0 \mod 2 \\ s_i & \text{, otherwise} \end{cases}$$

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:

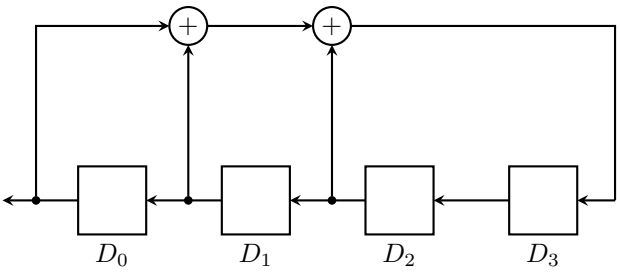
$$f'_s(x) = f_s(0^{|s|}) f_s(x)$$

is f'_s a PRF as well? Motivate your answer, again by describing the intuition behind it. In particular, if you don't think this is a PRF, you should show a successfull strategy for the distinguisher.

(c) **[4 points]** Explain how a pseudorandom genertor can be used to obtain an EAV-secure private-key encryption scheme. Why can't this scheme achieve CPA-security?

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

Consider the following LFSR:



(a) **[4 points]** Draw the cycle of the LFSR transition diagram obtained by starting from the initial state $(0, 0, 0, 1)$. What is the length of this cycle?

(b) **[3 points]** Consider the following Boolean function $f : \mathbb{F}_2^3 \to \mathbb{F}_2$ described by its truth table:

x_1	x_2	x_3	$f(x_1, x_2, x_3)$
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	1
1	0	0	1
1	0	1	0
1	1	0	1
1	1	1	0

Compute the Walsh coefficient for the vector $a = (1, 0, 1)$. Based just on this coefficient, what can we say about the nonlinearity of f (i.e. assume that this is the maximum absolute value in the Walsh spectrum of f)?

(c) **[3 points]** Briefly describe the combiner model for stream cipher. Could the LFSR in part (a) be used as part of this model? If not, why?

Exercise 4 – Block Ciphers [10 points]

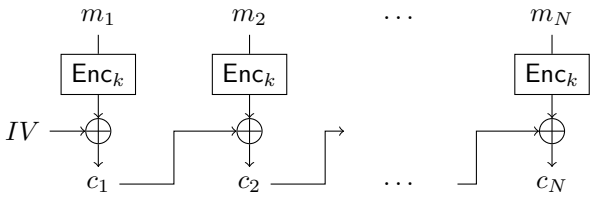
(a) [**5 points**] Briefly describe the SPN paradigm for designing a block cipher.

(b) [**2 points**] Name a block cipher that is designed following the SPN paradigm. What is the block length of this cipher?

(c) [**3 points**] What do block ciphers correspond to from a theoretical point of view? In particular, explain which pseudorandom object block ciphers are a good candidate of.

Exercise 5 – Block Ciphers and Modes of Operations

[10 points] Given a block cipher with block size n, we define the following mode of operation:



Where Enc_k denotes the block cipher encryption algorithm with key k, and IV is a (public) initialization vector in $\{0,1\}^n$.

(a) **[2 points]** Provide a formal description of the encryption algorithm, i.e. write the ciphertexts as a function of the plaintexts, key, and initialization vector.

(b) **[2 points]** Provide a formal description of the corresponding decryption algorithm, i.e. write the plaintexts as a function of the ciphertexts, key, and initialization vector. For this point, let Dec_k be the block cipher decryption algorithm with key k.

(c) **[6 points]** Discuss the security of this encryption scheme in detail.

Exercise 6 – MACs [10 points]

Unconditionally Secure MACs

Alice and Bob use an unconditionally secure MAC where $\mathcal{M} = \{0, 1, \cdots, 8\}$, $\mathcal{A} = \mathbb{Z}_{11}$ and $\mathcal{K} = \mathbb{Z}_{11} \times \mathbb{Z}_{17}$. The tag generation algorithm is defined for all keys $k = (i, j) \in \mathcal{K}$ and messages $m \in \mathcal{M}$ as:

$$\mathsf{Mac}_k(m) = (i + mj) \mod 11 \ .$$

(a) **[2 points]** Suppose that Alice and Bob chose the key $k = (3, 6)$, and Alice wants to send $m = 5$ to Bob. What is the corresponding tag?

(b) **[3 points]** Suppose that Alice and Bob use the same key to authenticate two messages. Specifically, Oscar observes the two consecutive message/tag pairs $(4, 1)$ and $(6, 9)$. What is the key k? Explain how Oscar can retrieve it, assuming that the tag generation algorithm is public.

Computationally Secure MACs

(c) **[3 points]** Let $F : \{0,1\}^* \times \{0,1\}^* \to \{0,1\}^*$ be a length-preserving pseudorandom function. Show that the following MAC based on F is not secure: Gen outputs a uniform n-bit string k, and to authenticate a message $m \in \{0,1\}^n$ we compute the tag as $t := \mathsf{Mac}_k(m) = F_k(m)||F_k(m_R)$, where m_R is the reverse of m. The verification algorithm is defined in the canonical way.

(d) **[2 points** What are the main differences between the CBC mode of operation for encryption and the CBC-MAC construction?

Exercise 7 – Hash Functions [10 points]

(a) **[3 points]** Suppose that we have a hash function $H : \{0,1\}^* \to \{0,1\}^{16}$. How many input messages do we need to hash before finding a collision with a probability of at least 50%?

(b) **[3 points]** Name an example of a standard cryptographic hash function, including its output length. Would it be feasible to perform a birthday attack with a success probability of at least 50%? Motivate your answer.

(c) **[4 points]** Provide a formal definition for the second preimage resistance property, by formulating a security game (similar to the one defined for collision resistance).

Exercise 8 – RSA Cryptosystem

[10 points] Alice wants to send a message to Bob using the RSA cryptosystem.

(a) **[4 points]** Bob creates an RSA key pair with primes $p = 5$ and $q = 7$, and public exponent $e = 5$. Compute the public and private key pair for Bob.

(b) **[4 points]** Alice encrypts the message $m = 5$. Compute the corresponding ciphertext.

(c) **[2 points]** Briefly explain how to make the basic RSA encryption scheme CCA-secure. In particular, do we need additional assumptions beside the hardness of factoring integers?

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

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

(a) [**5 points**] They agree on the multiplicative group $G = \mathbb{Z}_{19}^*$. Show that Alice and Bob can use $g = 2$ as a generator for G.

(b) [**3 points**] Manually execute the DH protocol between Alice and Bob, with secret exponents being respectively $a = 6$ and $b = 2$.

(c) [**2 points**] Beside its small size, is $p = 19$ a good choice for the security of the scheme? Motivate your answer.

Exercise 10 – Digital Signatures [10 points]

Alice wants to sign a message for Bob using the Digital Signature Algorithm (DSA).

(a) **[3 points]** Let the prime parameters be $p = 11$, $q = 5$, and let the generator be $g = 2$. Alice chooses a private signing key $x = 3$. Compute the corresponding public key y.

(b) **[4 points]** Alice wants to sign the message $m = 6$, with nonce $k = 1$. Use $H(m) = m$, and write down the signature pair (r, s).

(c) **[3 points]** In the standard DSA algorithm, what function H is used instead of $H(m) = m$? In this case, which additional assumption do we need beside the hardness of the discrete logarithm problem for the security of the scheme?