Introduction to Cryptography: midterm exam

Practice

Instructions: You can score a maximum of 50 points and you have 120 minutes to answer all five questions. Each question indicates how many points it is worth. You are **not** allowed to use any books/slides/notes/*etc.*, nor a smartphone or any device. Please write clearly and **explain your answers**. Each exercise is independent and they can be solved in the order of your choice. The formula sheet can be found attached at the end of the exam. Do not forget to **put your name and student number on each sheet.**

1. (**10 points**) **Symmetric cryptography open questions.**

   (a) Copy the following table and enter the cryptographic examples below it into your table in the correct columns (Not all the choices below have a place in the table!!!): 5 pt

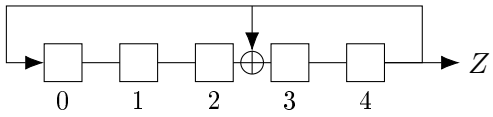
stream cipher	block cipher	MAC-function	hash function

   Choose from: *AES, DES, LFSR, CBC-MAC[AES], Combiner LFSR, Triple-DES, CBC-mode, ECB-mode, AES in CTR-mode, Filtered LFSR, SHA-3, sponge, MD5*

   (b) Copy and fill the following table. You can choose from the options *random permutation* and *(truncated) random oracle*. Each may appear more than once. 5 pt

Cryptographic scheme	Ideal version
Stream cipher	
Block cipher	
MAC-function	
Hash function	
XOF	

2. (**9 points**) **LFSR security** Consider the following linear feedback shift register.



   (a) Give the upper bound for the security strength when only considering exhaustive key search. 3 pt

   (b) Consider the output stream $Z = \texttt{10001}$. Determine the initial state of the LFSR. 6 pt

3. **(9 points) Message authentication code.** In this question, we are confronted with a bad MAC design. We have an n-bit key K. Let $\mathrm{B}_K \colon \{0,1\}^n \to \{0,1\}^n$ be a PRP secure block cipher. Consider messages m of length $3n$ bits. Write $m = m_1 \| m_2 \| m_3$ where $|m_1| = |m_2| = |m_3| = n$. The symbol $\|$ denotes concatenation of strings. Our MAC function is defined as:

$$\mathrm{MAC}_K(m) = \mathrm{B}_K(\overline{m_1}) \oplus \mathrm{B}_K(m_3) \| \, \mathrm{B}_K(\overline{m_2} \oplus m_3).$$

Consider a generation query of the form $m_1 \| 1^n \| m_3$, that provides you with the tag $T = t_1 \| t_2$.

(a) Give explicit expressions for t_1 and t_2. [Hint: Your expressions will likely use B_K.] 2 pt

(b) Show how you can make a forgery for this MAC function without making any other generation queries. [Show that a verification query on your forgery outputs that the tag is valid. Hint: You can distill more information from the generation query than just the values t_1 and t_2.] 7 pt

4. (**12 points**) **Distinguishing one-round Feistel.** In this exercise, we consider a one-round Feistel structure. Let $\mathrm{F}_K \colon \{0,1\}^\ell \to \{0,1\}^\ell$ be indistinguishable from a random permutation. We are going to show that this Feistel structure is not PRP-secure. In order to do this, we want to find a distinguisher $\mathcal{D}$ that has non-negligible advantage in distinguishing this Feistel structure from a random permutation.

(a) Give a distinguisher $\mathcal{D}$ that distinguishes the one-round Feistel structure from a random permutation. [Make sure that it will yield a non-negligible advantage in (c).] 4 pt

(b) What is the probability that your distinguisher guesses that it is talking to a one-round Feistel structure, while it is actually talking to a random permutation? 3 pt

(c) Give the advantage of your distinguisher. 3 pt

(d) Is this one-round Feistel structure SPRP-secure? 2 pt

5. (**10 points**) EMAES, **a new great block cipher! But how secure is it?**

In 1977, NIST standardized DES, and in 2001, they standardized its successor AES, so it looks like they will publish a successor to AES in 2025, and that would logically be called EMAES (an Even More Advanced Encryption Standard). We make some speculation on what that cipher will look like and ask you about its security strength against some attacks. We assume the following about EMAES:

- Its block length is 256 bits.
- Its key length is 150 bits.
- Its security goal is to be PRP secure. It is not designed to be SPRP secure.

(a) PRP and SPRP security are about distinguishing a block cipher from an ideal counterpart. Give that ideal counterpart and explain the difference between PRP and SPRP security. 2 pt

(b) Explain why PRP security is appropriate in counter mode and SPRP security in CBC mode. 1 pt

(c) How can you attack EMAES with exhaustive key search? Explain the attack mentioning online encryption queries and offline encryption queries. 2 pt

(d) Give the security strength of EMAES against exhaustive key search. 1 pt

(e) Explain how you can create a distinguisher for PRP security with the exhaustive key search attack. 1 pt

(f) Consider a *multi-target* attack: suppose we have d encryption devices, which implement EMAES with each a different secret key. The goal of the attacker is to find one of these keys. Give the security strength of EMAES against such an attack for $d = 1024 = 2^{10}$. 2 pt

(g) Give the maximum value of d for which EMAES still offers 128 bits of security against a multi-target attack with d targets. 1 pt