# ECE4802/CS4801

Final Exam D-23

Name: _____

| Problem | 1 | 2 | 3 | 4 | 5 | **Total** |
|---|---|---|---|---|---|---|
| | | | | | | |

**Exam rules:**

- Deadline: May 2, 2023, 11:59**am** - *No Extension!*.
- Submission: on Canvas
- Individual test: *No team work!*

Good luck and have fun!

1. ***Explain the followings:***

   (a) What is Kerckhoffs' Principle? Why is it important?

   (b) Define perfect secrecy and computational security. Explain why popular practical encryption schemes achieve computational security but not perfect secrecy.

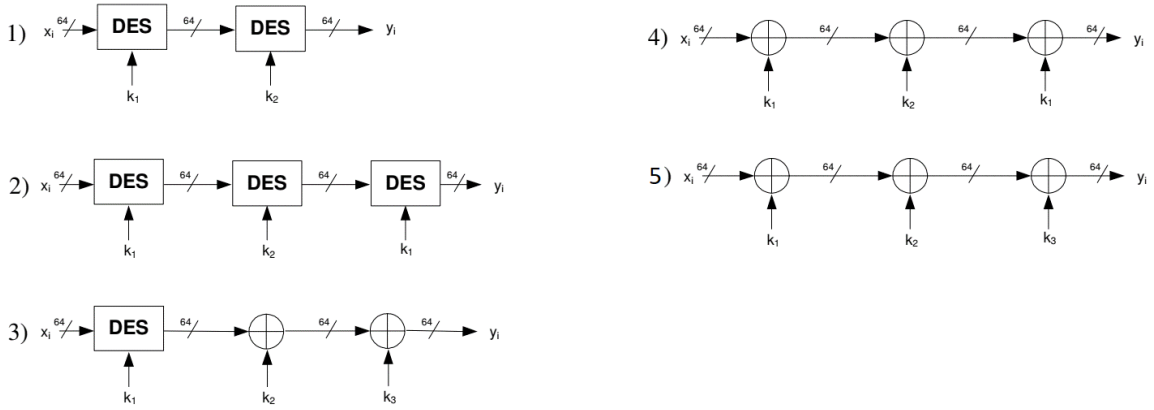
   (c) Explain the main differences between public (asymmetric) key and secret (symmetric) key schemes.

   (d) Explain the similarities and differences between public key encryption schemes and digital signature schemes.

2. ***DES***

   There are different ways to increase the security of block ciphers. This problem proposes different methods to increase the security against brute force attacks. Your task is to assess the security of these methods.

   Assume that the adversary knows two message-ciphertext pairs $(m_1, c_1)$ and $(m_2, c_2)$. Furthermore, the adversary is able to break a simple DES instance via a brute-force attack. The key lengths are $|k_1| = |k_2| = |k_3| = 64$ bit. The following schemes are given:




   (a) Explain how an adversary can efficiently attack the given encryption schemes (i.e.,explain the most efficient attack on the schemes brief and concisely).

   (b) What is the effective key length of the scheme, i.e., how many bits of the key does an attacker have to guess to break the scheme?

   (c) Which of the schemes show a significantly improved security compared to a single encryption?

3. *Elliptic Curve D-H Key Exchange*

   Alice and Bob want to share a key using D-H Key Exchange on Elliptic Curves. And, they choose the elliptic curve $E : y^2 = x^3 - x + 188 \; mod \; 751$ and a generator point $\alpha = (0, 376)$. Alice chooses $a_A = 2$ and Bob chooses $a_B = 3$ as the private key.

   (a) Find the public keys for Alice and Bob.

   (b) Using D-H Key Exchange, find the common key generated by Alice and Bob.

4. *Digital Signatures*

   Suppose we are not concerned with the confidentiality of our messages but about adversaries altering them during transmission. Assume we are using a 128-bit block cipher $E_k(\cdot)$, e.g. AES, to build integrity checks to detect if somebody tampered with our data during transmission. For instance, for a message $m$ we compute a tag $t = E_k(m)$ and send it along with the message as $(m, t)$ so that the recipient can verify the message by simply checking if $t \stackrel{?}{=} E_k(m)$.

   (a) Name one weaknesses of this scheme? (Hint: Consider the key $k$ for encryption.)

   (b) Propose a modification to the basic scheme to eliminate the weakness.

5. *Security Services for Protocols*

   We want to explore security services of *secrecy*, *integrity*, *authenticity*, and *non-repudiation* can be provided by the combination of different cryptographic primitives. The original message $m$ is being processed as described in the short protocols below. Then it is sent as data stream $y$ from one party to another (e.g., from Alice to Bob).
   To realize the protocols, a hash function $H(x)$, a message authentication code $MAC(x)$, a digital signature $Sign(x)$, a stream cipher $Enc_S(x)$ and a block cipher $Enc_B(x)$ are used.
   State which security services are provided by which protocol. Also give a *brief* explanation why security service is provided or not. When checking *integrity*, differentiate between random changes occurring during transmission via a noisy channel and deliberate changes introduced by an adversary.

   (a) $y = [H(m), m]$

   (b) $y = [MAC(m), m]$

   (c) $y = [Enc_S(H(m)), m]$

   (d) $y = Enc_B(m, H(m))$

   (e) $y = Enc_S(m, Sign(m_l))$, with $m_l$ being the last block of a message $m$.