ECE/CS578 Final Exam

Fall-23

Name: ________________________________

Problem	1	2	3	4	**Total**

Exam rules:

- Deadline: December 14, 2023, 11:59pm.
- 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.

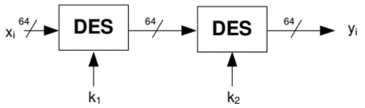
   (c) Explain the main differences between public key and secret key schemes.

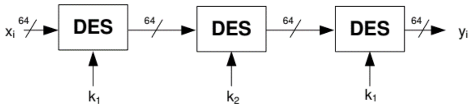
   (d) Explain the similarities and differences between public key encryption schemes and digital signature schemes.

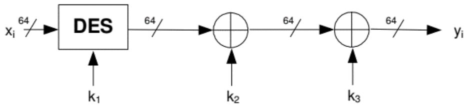
2. ***DES***

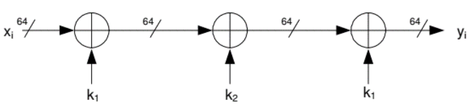
   There are different ways to increase the security of block ciphers. This problem proposes different methods to increase the security against brute force attacks. Your task is to assess the security of these methods.

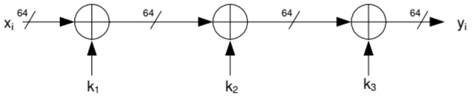
   Assume that the adversary knows two message-ciphertext pairs (m_1, c_1) and (m_2, c_2). Furthermore, the adversary is able to break a simple DES instance via a brute-force attack. The key lengths are $|k_1| = |k_2| = |k_3| = 64$ bit. The following schemes are given:

1)


2)


3)


4)


5)


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

   (b) What are the effective key length of the schemes, 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. ***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.

4. ***Triple RSA***

In class, we have seen that multi-encryption, i.e. cascading encryption functions, e.g. triple DES $\mathsf{TDES}_{k_1k_2k_3}(x) = \mathsf{DES}_{k_1}(\mathsf{DES}_{k_2}(\mathsf{DES}_{k_3}(x)))$ may be used to increase the security level of block ciphers.
Now consider the case, where we use multi-encryption on a public-key algorithm: RSA encrypt data multiple times with different keys, same modulus. Can we come to the same conclusion for RSA encryption? Mathematically justify your answer for triple RSA.