Module:	Level:	Exam:
Advanced Computer Systems Security	2nd Year Master (Distributed Architectures)	Regular Final Session
Unauthorized documents	Duration: 1 hour 30	Scientific calculator allowed

Monday, January 13, 2025 **Answer clearly and concisely**

Exercise 1 : 07 pts (Operation modes)

A plaintext M is divided into five blocks, $m_1, m_2, \ldots m_5$, encrypted with a symmetric cryptosystem and producing the encrypted blocks $c_1, c_2, \ldots c_5$. During transmission, errors affected some blocks.

1) What is the decryption result of each block c_i in each of the following scenarios ?
   (a) ECB "Electronic Code Book" operation mode and c_1 and c_3 are erroneous.
   (b) CBC "Cipher Block Chaining" operation mode and IV, c_2, and c_4 are erroneous.
   (c) CBC "Cipher Block Chaining" operation mode and only c_3 is erroneous.
   (d) CTR "Counter" operation mode and both c_1 and c_4 are erroneous.
2) Compare these three modes of operation according to 3 criteria of your choice.

Exercise 2 : 06 pts (Diffie–Hellman Key Exchange)

Ali and ***Omar*** agree to use the prime $p = 73$ and the base $g = 11$ for a Diffie–Hellman key exchange. ***Ali*** sends ***Omar*** the value $A = 19$ obtained using a secret exponent a. ***Omar*** asks your assistance, so you tell him to use the secret exponent $b = 10$.

1) What value B should ***Omar*** send to ***Ali*** ?
2) What is their shared secret value ? (Draw the corresponding timeline)
3) Can you easily figure out ***Ali***'s secret exponent ? (Consider the general case).

Exercise 3 : 07 pts (RSA Cryptosystem)

Ali uses an RSA system with $p = 137$ and $q = 151$.

1) Calculate the values of the RSA modulus N and $\varphi(n)$, the Euler's totient.
2) What is the smallest usable value of the encryption exponent e such that $e \leq 10$? Justify your answer.
3) What are ***Ali***'s public and private keys in this case ?
4) ***Omar*** wants to send securely the plaintext $m = 16$ to ***Ali***. What is the corresponding cryptogram c ?
5) What plaintext m corresponds to the cryptogram $c = 2$ sent by ***Omar*** to ***Ali*** ?

Yacine, a friend of ***Omar*** and ***Ali***, uses an RSA system with the same modulus N as ***Ali*** but with a different public exponent e', where $PGCD(e, e') = 1$. ***Salim*** (an intruder) captures c and c', the encryption of the same plaintext message m sent by ***Omar*** to ***Ali*** and ***Yacine***, respectively.

6) Show that ***Salim***, in this case, can easily determine the value of m.

Note: $2^{5100} \equiv 1 \mod 20687$ and $2^{1000} \equiv 17181 \mod 20687$