National University of Computer and Emerging Sciences
Lahore Campus

Information Security (CS3002)

Sessional-I Exam

Date: September 21st 2024

Course Instructor(s)

AK, AIS, MZH, SMI, AH, RAR

Total Time (Hrs): 1

Total Marks: 40

Total Questions: 4

____________ ____________ ________________________

Roll No Section Student Signature

Do not write below this line

Note: Students will also write the formula used in each calculation, no direct answer will be accepted. If you think some information is missing then make an assumption and write it clearly. Write all the answers including MCQs on the given answer sheet.

CLO-1	Explain key concepts of information security such as design principles, cryptography, risk management
CLO-2	Discuss legal, ethical, and professional issues in information security
CLO-3	Analyze real world scenarios, model them using security measures, and apply various security and risk management tools for achieving information security and privacy
CLO-4	Identify appropriate techniques to tackle and solve problems of real life in the discipline of information security
CLO-5	Describe issues related to ethics in the field of information security

CLO #: 1

Question No. 1: Choose the correct options(s). [5 marks]

1. What is the default access level to an object or resource according to fail-safe defaults?
   a. Read-only
   b. Write-only
   c. None
   d. Full access

2. Which mathematical operation is central to the security of the Diffie-Hellman algorithm?
   a. Matrix multiplication
   b. Modular exponentiation
   c. Symmetric encryption
   d. Factorization of large primes

3. In the DES algorithm the round key is __________ bit and the Round Input is ____________bits.

   a. 48, 32
   b. 64,32
   c. 56, 24
   d. 32, 32

4. Passwords and/or sensitive data are read by (unauthorized) third parties ___
   a. Sniffing Attack
   b. Spoofing Attack
   c. Identity Theft Attack
   d. Shadow Server

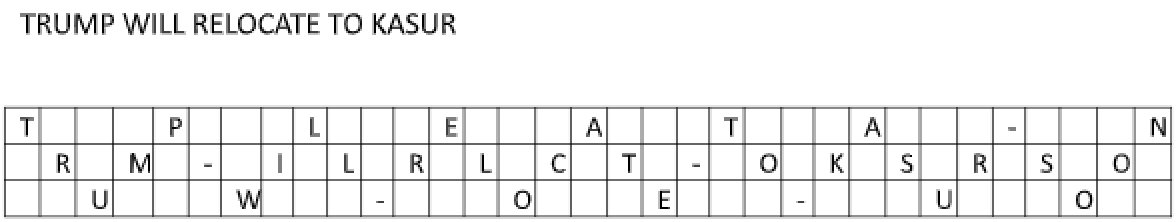
5. In the RSA algorithm, what is the relationship between the public and private keys?
   a. Both keys are identical
   b. The private key is the inverse of the public key modulo the totient ϕ(n)
   c. The public key is used for decryption and the private key for encryption.
   d. The private key and public key are randomly generated and unrelated.

CLO #: 1

Question No. 2 [5+5+5 marks]

A. Use the Rail Cipher to decrypt the following ciphertext, assuming a depth level of 3:

TPLEATA_NRM_ILRLCT_OKSRSOUW_OE_UO (5)



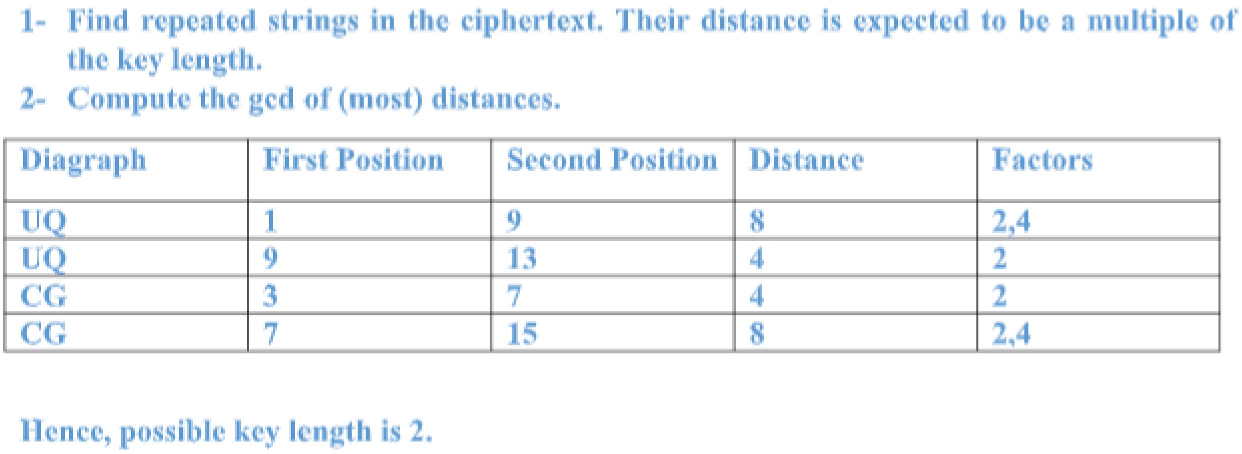
TRUMP WILL RELOCATE TO KASUR

T				P				L				E				A				T				A				-				N
	R		M		-		I		L		R		L		C		T		-		O		K		S		R		S		O	
		U				W				-				O				E				-				U				O		

B. The following message is encrypted using the Vigenère cipher.

UQCG OQCG UQSV UQCG

What possible length could the keyword have and why? (5)



1- **Find repeated strings in the ciphertext. Their distance is expected to be a multiple of the key length.**
2- **Compute the gcd of (most) distances.**

Diagraph	First Position	Second Position	Distance	Factors
UQ	1	9	8	2,4
UQ	9	13	4	2
CG	3	7	4	2
CG	7	15	8	2,4

Hence, possible key length is 2.

C. Encrypt the following plaintext **"samosa is ready"** using the Row Transposition Cipher, with key "**nick**" (if your roll number ends with an even digit) or key "**back**" (if your roll number ends with an odd digit). (5)

CLO #: 3

Question No. 3: [10+5 marks]

A. In the RSA algorithm, given that the **p = 61** and **q=53**. You need to calculate the following items:

1. The value of n. 3233
2. The totient ϕ(n). 3120
3. If the public exponent e=17 private key exponent d. 2753 (2+3+5)

B. Suppose Alice and Bob wish to perform Diffie Hellman key exchange. They agree on prime number p = 11 and generator g = 6. Alice chooses a secret 5, while Bob chooses 8. An attacker Mallory is listening to all of their communication. He chooses his own secret 4.

Show the calculation that proves that Mallory can perform a man-in-the-middle attack against Alice and Bob's key exchange. (5)

Alice public = 6^5 mod 11 = 10
Mallory public = 6^4 mod 11 = 9
Bob public = 6^8 mod 11 = 4

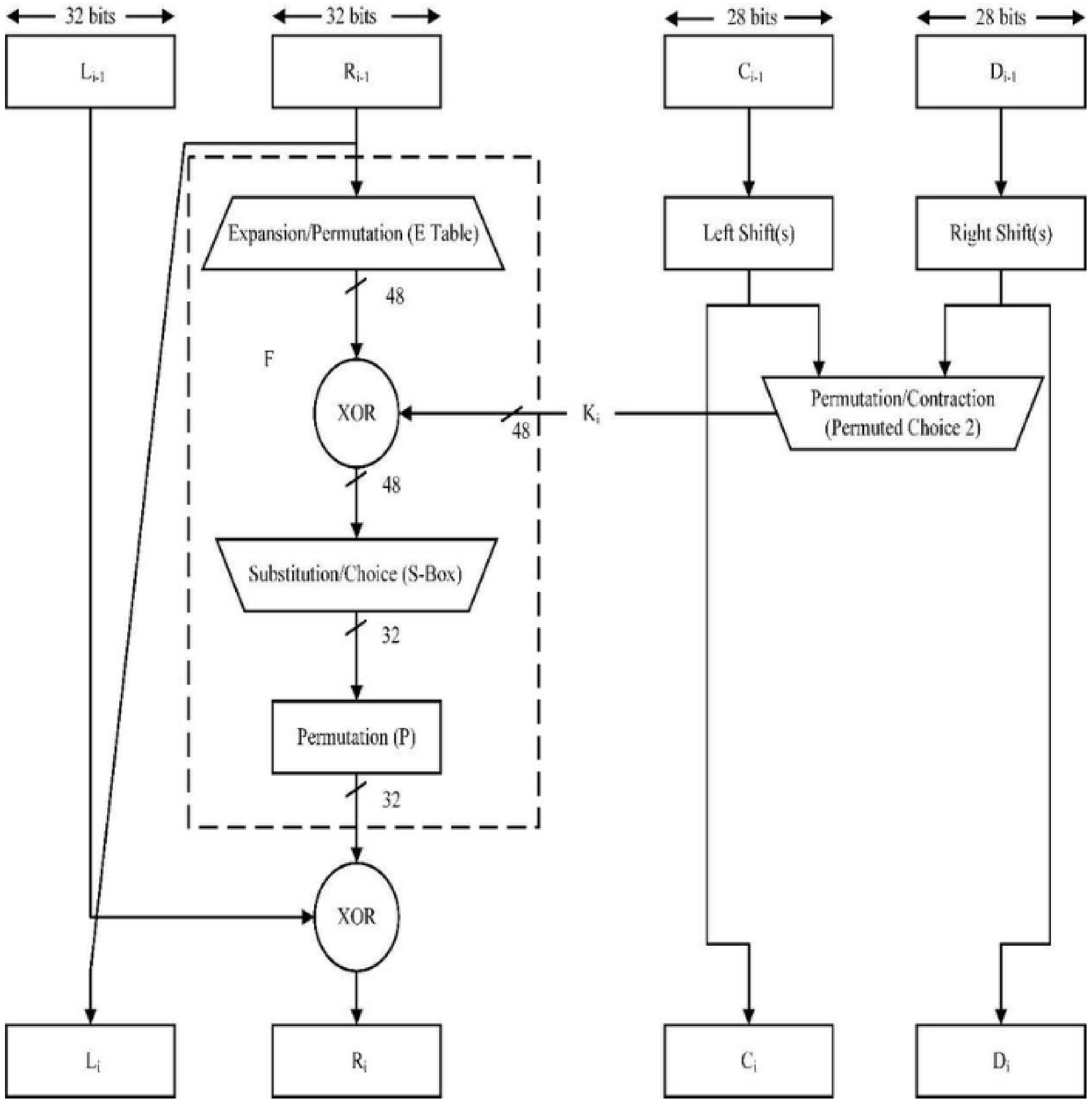
Key between Alice and Mallory
Alice calculates K 1 = 9^5 mod 11 = 1
Mallory calculates K 1 = 10^4 mod 11 = 1

Key between Bob and Mallory
Bob calculates K 2 = 9^8 mod 11 = 3
Mallory calculates K 2 = 4^4 mod 11 = 3

CLO #: 1

Question No. 4: [5 marks]

Draw the block diagram of a DES single round. Proper label the diagram.


32 bits
32 bits
28 bits
28 bits
L_{i-1}
R_{i-1}
C_{i-1}
D_{i-1}
Expansion/Permutation (E Table)
48
F
XOR
48
K_i
48
Substitution/Choice (S-Box)
32
Permutation (P)
32
XOR
Left Shift(s)
Right Shift(s)
Permutation/Contraction (Permuted Choice 2)
L_i
R_i
C_i
D_i