nd write it clearly.

Question 1: 32 [CLO:1] [5 marks]

1. The process of identifying vulnerabilities and threats and their impact and probability of occurring an attack is called ________.
   a. Vulnerability assessment
   b. Vulnerability identification
   c. Threat detection
   [✓ d.] Risk analysis ✓

2. Receiving an SMS message where the sender's number is fake, is an attack against ______.
   a. Confidentiality
   b. Integrity ✓
   c. Availability
   [✓ d.] Authenticity

4

3. Which are the most frequently found letters in the English language ?
   a. e,a
   b. e,o ✓
   [✓ c.] e,t
   d. e,i

4. Sam maintains a public key ring in his computer. He will pick a key from the ring during
   a. Asymmetric encryption
   b. Signing a message
   c. Asymmetric decryption ✗
   [✓ d.] Both a and c

∴ depends on the scenario whether user wants confidentiality or authentication.

5. In the DES algorithm the Round Input is 32 bits, which is expanded to 48 bits via __________
   [✓ a.] Scaling of the existing bits
   b. Substitution of the existing bits
   c. Addition of zeros ✓
   d. Addition of ones

[CLO: 3] [6+4 marks]

4

Question 2: Short Questions

Part I:

Identify the kind of attacks in each of the following statements and identify at least a couple of reasons the people fall for that

a. You receive a phone call. The caller claims that they are from a bank, and ask your debit card number and OTP for the purpose of account confirmation, otherwise your account will be blocked.

∴ Phishing Attack

- People are manipalated into thinking that there data is mandaiory and fall into this pit.

b. You tried to login to your flex account during which you ignored a warning displayed by the browser and later on you came to know that your login credentials have been stolen.

∴ Back Door Attack

- People usually dont pay attention to details of warnings.
- The hackers dont let the system to display appropriate warnings.

c. The outgoing network traffic of your system has suddenly increased and on diagnosis, you have identified that your system is constantly sending a specific request to a server.

∴ Denial of service

- It cause users to neglect the security and their overall system performance is affected because of that.

Part II:

Question: Using following Playfair matrix [CLO: 1] [4 marks]

M	F	H	I/J	K
U	N	O	P	Q
Z	V	W	X	Y
E	L	A	R	G
D	S	T	B	C

4

Encrypt this message:

"Must see you over Cadogan West. Coming at once."

Pairs:	MU	ST	SE	EY	OU	OV	ER	CA	DO	GA	NW	ES	TC	OM
Cipher :	UZ	TB	DL	GZ	PN	NW	LG	TG	TU	ER	OV	LD	BD	UH

Pairs:	IN	GA	TO	NC	EX
Cipher:	FP	ER	HW	QS	RZ

Cipher : UZ TB DL GZ PN NW LG TG TU ER OV LD BD UH FP ER HW QS RZ

0038

estion 3: [CLO:1] [2+4+4 marks]

a. Encrypt the text "voteforme" using Vigenère cipher with a key 245.

Text:	V	O	T	E	F	O	R	M	E
	2	4	5	2	4	5	2	4	5
cipher	24	19	25	7	10	20	20	17	10
→	X	S	Y	G	J	T	T	G	J

2

A	B	C	D	E	F		
1	2	3	4	5	6		
G	H	I	J	K	L	M	
7	8	9	10	11	12	13	
N	O	P	Q	R	S	T	U
14	15	16	17	18	19	20	21
V	W	X	Y	Z			
22	23	24	25	26			

b. Show the process of Diffie-Helman key exchange using a prime 47 and generator (α) 11. Suppose Alice chooses a secret 9 and Bob chooses 16.

$q = 47$

$\alpha = 11$

$X_A = 9$

$X_B = 16$

∴ Public key of A

$Y_A = (\alpha)^{X_A} \bmod q$

$= (11)^9 \bmod 47$

$Y_A = 38$

∴ Public key of B

$Y_B = (\alpha)^{X_B} \bmod q$

$= (11)^{16} \% 47$

$= [(11^1 \% 47) \times (11^2 \bmod 47) \times (11^4 \bmod 47) \times (11^8 \% 47) \times (11^1 \bmod 47)] \bmod 47$

$Y_B = 3$

4

Key calculations

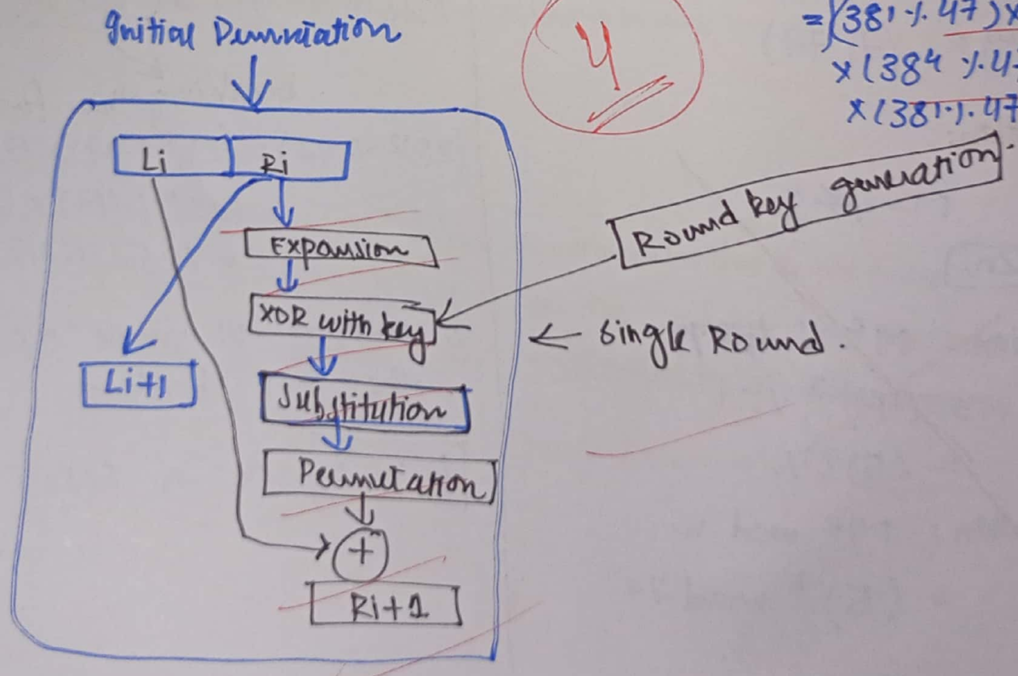
A: $(3)^9 \% 47 = 37$

B: $(38)^{16} \% 47 = 37$

↓

$= [(38^1 \% 47) \times (38^2 \% 47) \times (38^4 \% 47) \times (38^8 \% 47) \times (38^1 \% 47)] \% 47$

c. Draw the block diagram of DES single round.



4

Question 4: [CLO:1] [10 marks]

Describe the key development mechanism using RSA when the values of p and q are given to be 7 and 11 respectively? Although there are multiple options for choosing the encryption value 'e', let's choose 7 that fulfill the criteria and then find 'd' accordingly. You should provide all details and outcome should be written in the form of private and public keys. Demonstrate the working of your system by encrypting a number and then retrieving it back using decryption.

10

$p = 7$

$q = 11$

$n = (p\ q) = 77$

$\phi(n) = (p-1)(q-1) = 60$

$e = 7$

Now: $(d.e) \bmod 60 = 1$

$(d)(7) \bmod 60 = 1$

∴ Value of d by modulo inverse is 43

$(43)(7) \bmod 60 = 1$

$\boxed{d = 43}$

Private key: (43, 77)

Public key: (7, 77)

∴ Encryption:

suppose $M = ~~47~~\ 5$

$\boxed{M < n}$

~~Encryption: $M^e \% 77$~~

~~$= (47)^7 \%$~~

~~$= (5)^7 \%$~~

~~Encryption: $M^e \bmod n$~~

~~$= (5)^7 \bmod 77$~~

∴ Encryption

suppose $M = 3$ $(m < n)$

∴ $M^e \% n$

$= (3)^7 \% 77$

$= \boxed{25}$

∴ Decryption

$= (25)^{43} \% 77$

$= [(25^1 \% 47) \times (25^2 \% 47) \times$

$(25^4 \% 47) \times (25^8 \% 47) \times$

$(25^{16} \% 47) \times (25^{12} \% 47)] \% 47$

breaking this further.

$(25^{12} \% 47) = (25^1 \% 47) \times (25^2 \% 47) \times$

$(25^4 \% 47) \times (20^4 \% 47)$

$\times (25^1 \% 47)$.

∴ solving all above we get the text back:

$\boxed{D = 3}$ as a result.