Manav_19-1015A

Assignment -1

Q.1. Perform encryption and decryption using RSA algorithm

a. $P = 5, q = 11, e = 3, m = 9$

→ 1. $n = p \times q = 5 \times 11 = 55$

2. $\phi(n) = (p-1) \times (q-1) = 4 \times 10 = 40$.

3. Since e is already given $= 3$

4. To find d.

$$d = \frac{(K * \phi(n) + 1)}{e} \quad \text{for some integer } K.$$

Let us take $K = 2$.

$$\therefore d = \frac{2 \times 40 + 1}{3} = 27$$

4. To find d.

Using equation

$ed \bmod \phi(n) = 1$

$\therefore 3 \times d \bmod 40 = 1$

$\therefore d = 27$.

5. Public key → (3, 55)

private key → (27, 55)

6. $m = 9$.

∴ Encryption

$C = m^e \bmod n = 9^3 \bmod 55 = 14$

∴ Decryption

$P = C^d \bmod n = 14^{27} \bmod 55 = 9$

b) $p = 7$, $q = 11$, $m = 8$

→ 1. $n = p \times q = 7 \times 11 = 77$

2. $\phi(n) = (p-1)(q-1) = 6 \times 10 = 60$

3. To find e

$1 < e < 60$ and $\gcd(e, \phi(n)) = 1$

$\therefore e = 7$

4. To find d.

$ed \bmod \phi(n) = 1$.

$\therefore 7 \times d \bmod 60 = 1$

$\therefore d = 43$

5. Public key → $(7, 77)$

Private key → $(43, 77)$

6. $m = 8$

Encryption

$c = m^e \bmod n = 8^7 \bmod 77 = 57$

Decryption

$p = c^d \bmod n = 57^{43} \bmod 77 = 8$

c. $p = 11$, $q = 13$, $e = 11$, $m = 7$

→ 1. $n = p \times q = 11 \times 13 = 143$

2. $\phi(n) = 10 \times 12 = 120$

3. Since 'e' is already e

$\therefore e = 11$

4. To find d

$ed \bmod \phi(n) = 1$

i.e. $11 \times d \bmod 120 = 1$

$\therefore d = 11$

5. Public key → (11, 143)

Private key → (11, 143)

6. $m = 7$

Encryption

$c = m^e \bmod n = 7^{11} \bmod 143 = 106$

Decryption

$p = c^d \bmod n = 106^{11} \bmod 143 = 7$

d. $p = 17$, $q = 31$, $e = 7$, $m = 2$

→ 1. $n = p \times q = 17 \times 31 = 527$

2. $\phi(n) = (p-1)(q-1) = 16 \times 30 = 480$

3 Since 'e' is already given

i.e $e = 7$

4. To find d

$ed \bmod \phi(n) = 1$

$\therefore 7 \times d \bmod \phi(n) = 1$

$\therefore d = 343$

5. Public key → (7, 527)

Private key → (343, 527)

d.

→ Encryption. $m = 2$

$c = m^e \bmod n = 2^7 \bmod 527 = 128$

Decryption.

$P = c^d \bmod n = 128^{343} \bmod 527 = 2.$

e. $P = 17, \ q = 37, \ m = 2$

→ 1. $n = P \times q = 17 \times 37 = 629$

2. $\phi(n) = (P-1)(q-1) = 16 \times 36 = 576$

3. To find e.

$1 < e < \phi(n)$ and $\gcd[e, \phi(n)] = 1$

$\therefore e = 7$

4. To find d

$ed \bmod \phi(n) = 1$

$7 \times d \bmod 576 = 1$

$\therefore d = 247$

5. Public key → (7, 629)

Private key → (247, 629)

6. $m = 2$

Encryption

$c = m^e \bmod n = 2^7 \bmod 629 = 128$

Decryption

$P = c^d \bmod n = 128^{247} \bmod 629 = 2.$

Q.2.

→ $n = 35$, $e = 5$, $c = 10$

Soln

Since

1. $n = 35 = p \times q$

$\therefore p \times q = 7 \times 5$

$\therefore p = 7$

$q = 5$

2. $\therefore \phi(n) = (p-1)(q-1) = 6 \times 4 = 24$

3. Since e is already given

i.e $e = 5$

4. To find d

$ed \bmod \phi(n) = 1$

$\therefore 5 \times d \bmod 24 = 1$

$\therefore d = 5$

5. Public key → (5, 35)

Private key → (5, 35)

6. Now, $c = 10$ and $m = ?$

$c = m^e \bmod n$

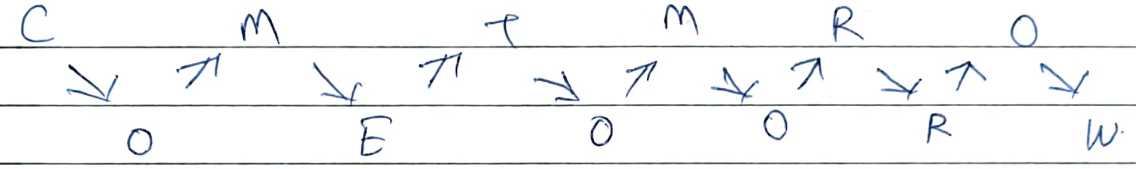
i.e $10 = m^5 \bmod 35$

$\therefore m = 5$

Q3.

→ Given cipher text - CMTMROOEOORW

Considering key = 2



∴ The plain text is COME TOMORROW

Q.7.

→

	Substitution Cipher	Transposition Cipher
1.	Each Character replaced with other Character	Each character positioned differently from original position
2.	mono alphabetic and poly alphabetic are its two forms	key-less and keyed are its two forms
3.	Character identity is changed but position is same	Character position is changed but identity is same
4.	A letter less frequently used can be easily traced	A letter near to original position get traced easily.
5.	Caesar cipher is an Example	Rail-Fence cipher is an example

Q.8

→

	Steganography	Cryptography
1.	It is a technique to hide the existence of communication	It is a technique to convert the secret message into other readable form
2.	It is a kind of hidden communication	It is a kind of known communication.
3	It does not alter the structure of data	It alters the structure of data.
4.	The final result obtained is stegomedia	The final result obtained is cipher text
5.	Attack's name is. Steganalysis	Attack's name is cryptanalysis.

Q.13

→

	Symmetric cryptography	Asymmetric cryptography
1.	It requires a single key.	It requires two keys
2	Encryption is fast	Encryption is slow
3.	Size of cipher text is same or small than the original	Size of cipher text is same or large than the original
4.	It is used to transfer large amount of data	It is used to transfer small amount of data
5	Resource utilization is low.	Resource utilization is high
6.	Ex. AES, DES	Ex. RSA

Q.4

→ Plaintext : SWARAJ IS MY BIRTH RIGHT

Keyword : MONARCHY

Constructing 5×5 matrix.

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

Converting plain text to diagraphs

SW AR AJ IS MY BI RT HR IG HT

Now, Encipherment

QX RM BS SX NC IS DZ DO KI DP

∴ The encrypted text is

QXRM BSSX NCI SDZ DO KI DP

Q.5.

→ Decrypt - YMJTY.MJWX NIJTIC XNQJSHJ

method - ~~cts~~ Caesar Cipher

K = 5.

We use the formula for decryption as

$P = (C-K) \bmod 26$ where K=5

Y→24	(24-5) mod 26	19→T
M→12	(12-5) mod 26	7→H.
J→09	(9-5) mod 26	4→E
T→19	(19-5) mod 26	14→O.
Y→24.	(24-5) mod 26	19→T
M→12	(12-5) mod 26	7→H.
J→09	(9-5) mod 26	4→E
W→22	(22-5) mod 26	17→R
X→23	(23-5) mod 26	18→S
W→13	(13-5) mod 26	8→I
I→08	(8-5) mod 26	3→D
J→09	(9-5) mod 26	4→E
T→19	(19-5) mod 26	14→O
I→10	(10-5) mod 26	5→F
X→23	(23-5) mod 26	18→S
W→13	(13-5) mod 26	8→I
Q.→16	(16-5) mod 26	11→L
J→19	(9-5) mod 26	4→E
S→18	(18-5) mod 26	13→N.
H→07	(7-5) mod 26	2→C
J→09.	(9-5) mod 26	4→E

∴ The plaintext is "The Other side of Silence"

Q.6

→ Encrypt - Explanation
method - vigenere cipher
key - leg

Formula of encryption is.
$C_i = (P_i + K_i) \bmod 26$

Plain text	E	x	P	L	A	N	A	T	I	O	N
P's value	4	23	15	11	0	13	0	19	8	14	13
key stream	L	E	G	L	E	G	L	E	G	L	E
K's value	11	4	6	11	4	6	11	4	6	11	4
C's value	15	1	21	22	4	19	11	23	14	25	17
Cipher text	P	B	V	W	E	T	L	X	O	Z	R

Q.14. Explain AES along with its major attributes.

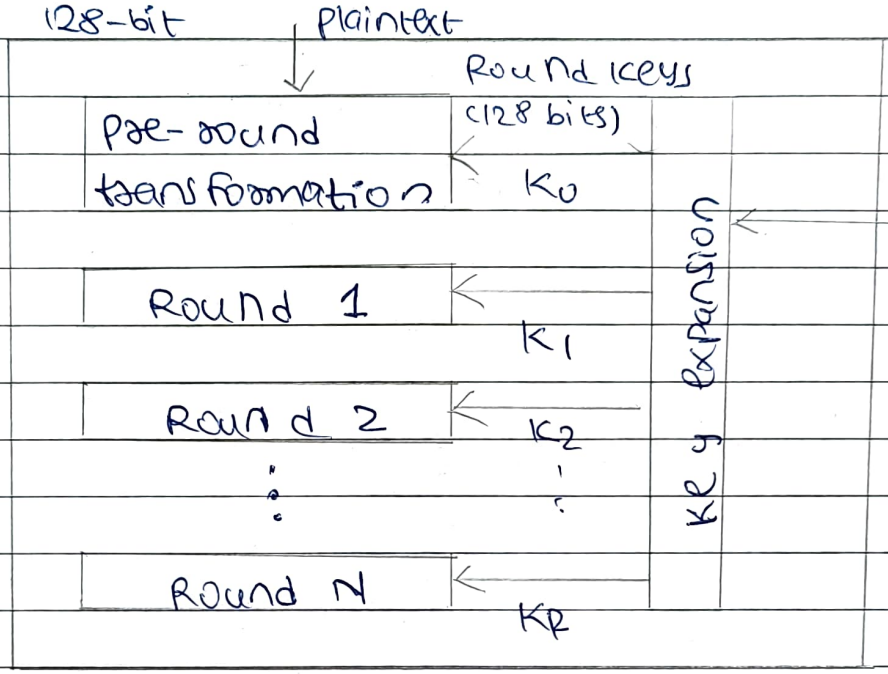
→ 1. AES is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST) in December 2001

2. AES is a non-Feistel cipher that encrypts and decrypts a data block of 128 bits. The number of rounds in AES is variable and depends on length of key.

3 Every version uses different key size, which can be 128, 192, or 256 bits, depending on number of rounds but the round keys are always 128 bits.

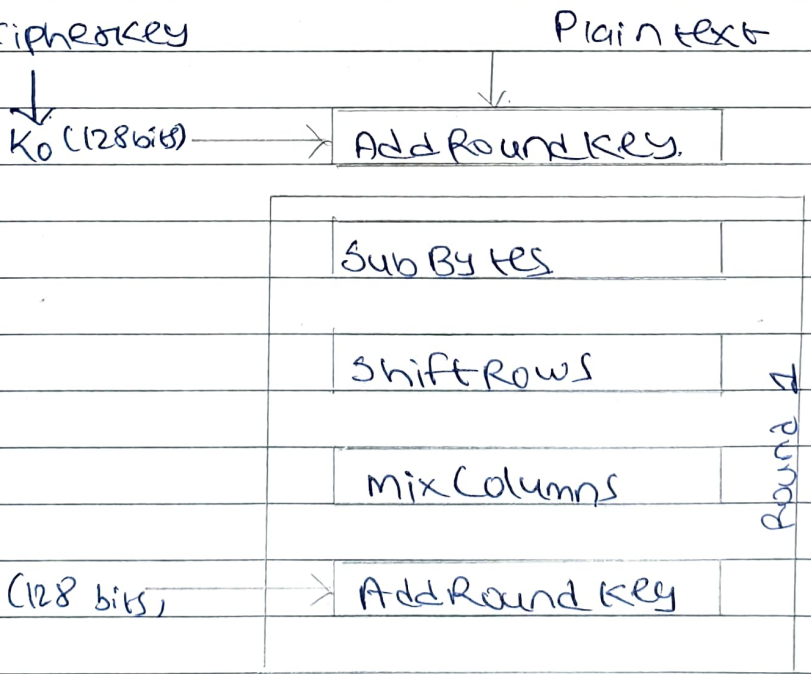
4. AES performs all its computations on bytes rather than bits. Hence AES treats 128 bits of plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing.

AES Diagrams



AES encryption cipher

b



Q.14.

→ 5. Encryption process:

a. At encryption site, each round comprises of four transformations that are invertible. The transformations are:

1. Sub Bytes (substitution)
2. Shift Rows (permutation)
3. mix columns (mixing)
4. Add Round key (key adding)

b. The pre-round section uses only one transformation (AddRoundKey). The last round has only three transformations and, mix columns transformation is not used.

6. Decryption Process:

a. The process of decryption of an AES ciphertext is similar to the encryption process in reverse order. At the decryption site, each round consists of four processes conducted in reverse order:

1. Add Round key (self-invertible)
2. InvMixColumns
3. Inv Shift Rows
4. Inv Sub Byte.

7. Key expansion:

a. AES uses a key-expansion process to create round keys for each round. If number of rounds is Nr, the key-expansion routine creates Nr + 1 128 bit round keys from one single 128-bit cipher key.

Q15. Explain different block cipher modes of operation.

→ There are five types of operations in block cipher modes:

1. Electronic Code Block (ECB) mode - block cipher
2. Cipher Block chaining (CBC) mode - block cipher
3. Cipher Feedback (CFB) mode - block ciphers acting as stream cipher
4. Output Feedback (OFB) mode - block cipher acting as stream ciphers
5. Counter (CTR) mode - block cipher

1. Electronic code Book (ECB) mode

a. Electronic code Book is the simplest mode of operation of block cipher. It works on processing a series of sequentially listed message blocks but 64-bit block at a time. Each block is separately encrypted.

b. Generally a message is larger than 64 bits in size, it can be broken down into series of blocks and the encryption procedure is repeated. Each block is encrypted using same key.

c. Because the same key used for all the blocks, ECB is used for an only small message.

Encryption : $C_i = E_K(P_i)$

Decryption : $P_i = D_K(C_i)$

Q15

3. 2. Cipher Block chaining (CBC) mode

a. CBC can be called as advancement of ECB. Here, at sender side, plain text is divided into blocks.

b. In this mode, Initialization vector (IV) is used which can be random block of text. IV is used to make the ciphertext of each block unique since the key used is same.

c. For encryption the first block and IV is combined using XOR operation and then the resultant message is encrypted using the key.

d. For decryption, at receiver side, ciphertext is divided into blocks. The first block is decrypted using same key, which is used for encryption. The resultant is XOR with IV to get plain text.

Encryption	Decryption
$C_0 = IV$	$C_0 = IV$
$C_i = E_K(P_i \oplus C_{i-1})$	$P_i = D_K(C_i) \oplus C_{i-1}$

3. Cipher feedback (CFB) mode

a. In this mode, data is encrypted in the form of units where each unit is 8 bits. Here, in order to encrypt the next plain text block, the cipher is given as feed back to next block of encryption with some new specifications.

Q.15

→ b Encryption:

$C_i = P_i \oplus \text{selectLeft}_r \{ E_{lC}[\text{shiftLeft}_r(S_{i-1}) \mid C(i-1)] \}$

Decryption:

$P_i = C_i \oplus \text{selectLeft}_r \{ E_{lC}[\text{shiftLeft}(S_{i-1}) \mid C(i-1)] \}$

E:- Encryption
Si = Shift register
Ci - ciphertext block i
lC - secret key
D - Decryption
P - Plaintext block i
T - Temporary register
IV - Initial vector (S1)

4. Output Feedback mode (OFB):

a. The OFB mode follows nearly same process as CFB mode except that it sends the encrypted output as feedback for next stage of encryption process instead of actual cipher which is XOR output.

b Plain text and leftmost 8 bits of encrypted IV are combined using XOR to produce the ciphertext. For the next stage, the ciphertext, which is the form in previous stage, is used as an IV for next iteration.

5. Counter (CTR) mode:

a. The CTR is a simple counter-based block cipher implementation. It uses the sequence of numbers as an input for the algorithm.

b. Every time a counter initiated value is encrypted and given as input to XOR with plaintext which results ciphertext.

Q.16. Explain Rootkits and its types.

→ 1. A rootkit is a covert computer program designed to provide continued privileged access to a computer while actively hiding its presence.

2. Root refers to the Admin account on Linux system and kit refers to software component.

3. This malicious software alters the regular functionality of OS on a PC in a stealthy manner.

4. There are also good uses of rootkits like a honeypot to detect attacks to enhance emulation software, to enhance security software for digital right management enforcement and device anti-theft protection.

Q.17. Explain DDOS attack.

→ 1. An additional type of DOS attack is Distributed Denial of service (DDOS) attack. In a DOS attack, it's one system that is sending the malicious data or requests, a DDOS attack comes from multiple system at once.

2. DDOS attackers often leverage the use of botnets. Attackers take advantage of security vulnerabilities or device weakness to control numerous devices using command and control software

Q.18 Explain various countermeasures against social Engineering attacks from individual user perspective and Organizational perspective.

⇒. The countermeasures can be:

1. Don't open emails and attachments from suspicious sources
2. Use multifactor authentication
3. Beaware of tempting offers
4. Keep your antivirus software updated
5. Continuously monitor critical system
6. Check SSL certificate
7. Penetration Testing

1. Don't open emails and attachments from suspicious sources - If you don't know the sender, you don't need to answer an email. Even if you know then and are suspicious about their message, CROSS-check and confirm the news from other sources such as via telephone.

2. Use multifactor authentication - One of most valuable pieces of information attackers seeks are user credentials. Using multifactor authentication helps ensure your account's protection in the event of system compromise.

3. Beaware of tempting offers - If an offer sounds too exciting, think twice before accepting it as fact.

4. Keep your antivirus software updated - make sure automatic updates are engaged or make it a habit to download the latest signatures first thing each day. Periodically check to make sure that the updates have been applied and scan your system for possible infections.

5. Continuously monitor Critical System - Make sure your system which houses sensitive information is being monitored 24x7. Scanning both external and internal systems with web application scanning can help to find vulnerabilities in system.

6. Check SSL certificate - Encrypting data, emails and communication ensure that even if hackers intercept your communication, they can't be able to access the information contained within. This can be obtained by obtaining SSL certificate.

7. Penetration Testing - The most effective approach among the ways to prevent social engineering attacks is conducting a pen-test to detect and try to exploit vulnerabilities in your organization.