Assignment 1

① What is cryptography, cryptology and cyrptanalysis?

⇒ The word cryptography comes from two Greek words "Cryptos" and "Graph" meaning "secret writing" and is the art and science of information hiding. In other words, Cryptography can be defined as the practice and study of secure communication techniques that protect information from third parties (adversaries).

Cryptanalysis is the breaking of codes. It encompasses all of the techniques to recover the plaintext and lor key from the ciphertext.

The combined study of cryptography and cryptanalysis is known as cryptology.

② What are different features/services/objectives provided by cryptography?

Cryptography provides several key security services to ensure safe communication and data protection. These include:

(i) Data Confidentiality: It ensures that information is accessible only to authorized users.

(ii) Data Integrity: It guarantees that data is not altered during transmission or storage.

(iii) Authentication: It confirms the identity of users or systems in communication.

(iv) Non repudiation: It prevents senders or receivers from denying that they sent or received a message.

(v) Access Control: It ensures only authorized users can access specific information or resources.

③ What is CIA traid? Explain.

The CIA traid is a fundamental model in cybersecurity and cryptography that defines three core principles for protecting information:

i) Confidentiality: It ensures that sensitive information is accessible only to authorized users. It is achieved through encryption, access control, & authentication mechanisms.

ii) Integrity: It ensures that data remains accurate and unaltered during storage or transmission. Integrity mechanisms fall into two classes; prevention mechanisms and detection mechanisms.

iii) Availability: It ensures that data and services are available when needed. It is achived through redundancy, failover mechanisms and network security measures.

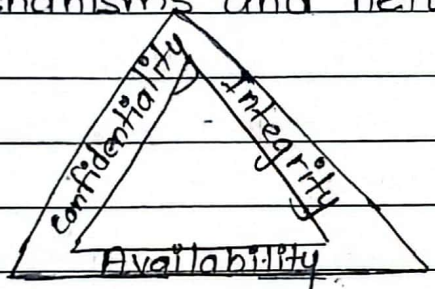

fig: CIA traid

The CIA triad is important as it provides a structured approach to security in cyptography and cybersecurity. It balances the three principles to maintain a secure and functional system.

④ Differentiate between active and passive attack with explanations of each category.

⇒ The differences between active and passive attack are as follows:

Features	Active Attack	Passive Attack
Definition	An attack where the attacker modifies, disrupts or injects data into a system.	An attack where the attacker only observes or monitors data without altering it.
Objective	To alter or damage system operations.	To secretly gather information.
Data Modification	Yes, data is modified or injected.	No, data remains unchanged.
Detection	Easier to detect because it disrupts normal operations.	Harder to detect as it does not alter data.
Prevention Methods	Firewalls, IDS/IPS, Encryption, authentication.	Encryption, traffic monitoring, access control.

(2)

(*) Active Attack: It can be subdivided into four categories:

(1) Masquerade attack: Here, an attacker pretends to be a legitimate user by using stolen credentials or exploiting security loopholes.

(2) Replay Attack: Here, the attacker captures and retransmits legitimate message to gain unauthorized access.

(3) Modification of Messages: The attacker alters message being transmitted between two parties.

(4) Denial of Service Attack: The attacker overwhelms a system or network to make services unavailable.

(*) Passive Attack: The two types of passive attacks are:

(1) Release of Message Contents: The attacker eavesdrops on and reads confidential messages.

Traffic Analysis: The attacker monitors communication patterns to gather intelligence without reading the actual content.

Explain message authentication and entity authentication.

Message Authentication ensures that a message has not been altered during transmission and that it comes from a legitimate source. It prevents message tampering, forgery and replay attacks. Techniques for message authentication are: Message Authentication Code, Digital Signatures, Hash functions. ~~Example: A bank sends a transaction confirmation to a customer with an HMAC.~~

Entity authentication verifies the identity of a user, device or system before granting access or communication rights. It prevents impersonation, unauthorized access. Types of entity authentication are: password-based authentication, challenge-Response authentication, Biometric authentication, Public Key authentication.

① Example of Message Authentication:

A bank sends a transaction confirmation to a customer with an HMAC. The customer's system verifies the HMAC to ensure the message is legitimate and has not been tampered with.

② Example of Entity Authentication:

A user logs into their online banking account. The system verifies their identity using a password and a one-time OTP (challenge-response authentication).

⑥ What is Repudiation? Explain types of repudiation and counter measures of it.

⇒ Repudiation refers to a situation where a user denies performing an action, such as sending a message, making a transaction or accessing data. It is a security threat.

Types of Repudiation:

① Message Repudiation: The sender of a message denies that they sent it.

② Transaction Repudiation: A user denies initiating or authorizing a transaction.

③ Data Access Repudiation: A user denies accessing or modifying data.

The counter measures to prevent repudiation are:

① Digital Signature: It uses asymmetric cryptography to sign messages providing proof of origin.

② Message Authentication Codes (MACs): - It is cyptographic hash-based verification that ensures a message has not been altered.

③ logging and Audit Trails: It maintain logs of user activities to track actions and provide evidence.

④ Timestapping: It adds a timestamp to messages or transactions prevents backdating or denial.

⑤ Non-Repudiation Services

⑥ Multi-factor Authentication (MFA)

⑦ What are security services and mechanisms.

⇒ Security services is a processing or communication service that enhances the security of the data processing systems and the information transfers of an organization.

They provide protection against various threat and vulnerabilities. Security services include following services:
⊙ Authentication ⊙ Access Control ⊙ Data Confidentiality
⊙ Data Integrity ⊙ Non repudiation ⊙ Availability service.

Security Mechanisms is process or a device incorporating such a process that is designed to detect, prevent, or recover from a security attack. They are used to preserve security in every system and make the system consistent. The security mechanisms are divided into:

(i) Specific Security mechanisms: Those that are implemented in a specific protocol layer, such as TCP or an application layer protocol.

(ii) Pervasive Security mechanisms: Those that are not specific to any particular protocol layer or security service.

(8) Differentiate conventional (symmetric) from public key (asymmetric).

⇒ The differences between conventional and public key are:-

Feature	Conventional (Symmetric) Cryptography	Public key (asymmetric) cryptography
Key Usage	Uses a single secret key for both encryption and decryption.	Uses a pair of keys; a public key for encryption and a private key for decryption.
Key Distribution.	Requires a secure channel to share the secret key.	The public key can be freely shared, reducing the need for secure key exchange.
Speed	Faster due to simpler algorithms.	Slower due to complex mathematical operations.

Feature	Conventional	Public key
Security	less secure if the secret key is compromised.	More secure, as the private key remains confidential.
Scalability	Not scalable for larger networks.	More ~~seab~~ scalable.
Use Cases	Used for encrypting large amounts of data like disk encryption and VPNs.	Used for secure key exchange, digital signatures and authentication.
Common Algorithms	AES, DES, 3DES, etc.	RSA, Diffie-Hellman, etc.

From above, It can be concluded that Symmetric Cryptography is ~~effecti~~ efficient for bulk data encryption but requires secure key exchange and Asymmetric Cryptography is useful for secure communications and authentication but is computationally intensive.

(9) Define the term keyspace. Justify the statement "larger the keyspace, higher the security."

⇒ A keyspace refers to the total number of possible keys that can be used in a cryptographic algorithm. It is determined by the length of the key and the number of possible values for each key component.

For eg: In a symmetric encryption algorithm with a 128-bit key, the keyspace consists of 2^{128} possible keys.

A larger keyspace means more possible keys, making brute-force attacks (trying all possible keys) practically impossible. Similarly a larger keyspace means more randomness and unpredictability, making it more difficult

for attackers to guess or predict the correct key. Also, some attacks exploit patterns in small keyspaces while A larger keyspace minimizes these vulnerabilities i.e. larger keyspace enhance protection against cryptoanalysis. In conclusion, a larger keyspace directly correlates with higher security, as it exponentially increases the difficulty for attackers to find the correct key. Hence, "Larger the keyspace, higher the security.

(10) Name any 6 block cipher schemes with their key sizes.

⇒

Block Cipher Algorithm	Key Sizes (in bits)
Data Encryption Standard (DES)	56-bit
Triple DES (3DES)	112 bit or 168 bit
Advanced Encryption Standard (AES)	128 bit, 192 bit, 256 bit
Blowfish	32-bit to 448 bit
Twofish	128 bit, 192 bit, 256 bit
Camellia	128 bit, 192 bit, 256 bit

(11) What should be considered while selecting a size of a block?

⇒ The block size in a block cipher determines how much data is encrypted at a time. Here are key factors to consider when selecting the block size:

(1) Security strength: Larger block sizes (Eg: 128-bit) provide better security against birthday attacks & coode book attacks.

(2) Performance & Efficiency: larger block sizes provide stronger security but may increase processing time & memory usage. Smaller block sizes require less computational power and memory, making them suitable for resource-constrained devices.

③ Data padding Overhead: If the data is not a multiple of the block size, padding is required. A larger block size means more padding overhead for small data.

④ Mode of Operation Compatibility: Different modes of operation handle block size differently. Some modes, like CTR, work efficiently with larger blocks.

⑤ Suitability for Different Applications: 128-bit block ciphers are widely used today due to their balance between security and efficiency.

⑫ Encrypt the message "attack from south east" with key 'point' using vigenere cipher.

⇒ Since Vigenere Cipher is a repeating key cipher, we repeat "Point" until it matches the length of the plain text.

Plaintext: ATTACKFROMSOUTHEAST

Key: POINTPOINTPOINTPOIN

Now we create a 26x26 table ~~where top row contains~~ (top row contains A-Z, left column A-Z & each row represent a shift of alphabet based on the left column letter) which has key letters on top, plaintext letter on the left. ~~Now~~ Then, we find the position of the plaintext letter in a column, corresponding to the key letter of the table and then taking the label of the row in which it appears as the ciphertext letter. This process continues until we find the ciphertext letters for all the ciphertext letters.

Doing So, the final Ciphertext is

Encrypted Text: "PHBNVZTZBFHCCGAIOAG"

(13) Encrypt the message "hide money" with key 'tutorials' using polyalphabetic cipher.

⇒ The polyalphabetic cipher (like Vigenere Cipher) uses multiple shifting alphabets based on a keyword. Here, we will use "TUTORIALS" as the key.

Plaintext: HIDEMONEY

KEY : TUTORIALS

Now, using the Vigenere Cipher, we get:

Ciphertext: ACWSDWNPQ

(14) Encrypt the plaintext "I study Cryptography" with the key 'guys' using playfair Cipher.

⇒ Here: Plaintext: Istudy Cryptography

Key: Guys

(i) Creating 5x5 playfair Matrix

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

(ii) Breaking plaintext into letter pairs, inserting "x" if needed (no double letters allowed in a pair):

"IS TU DY CR YP TO GR AP HY

(iii) Encrypting using playfair Rules:

IS: LU, TU: VG, DY: KD, CR: FO, YP: DW

TO: VN, GR: AN, AP: YR, HY: KG

⊙ Final encrypted Message is: LUVGKDFODWVNANYRKG

(15) Encrypt the plaintext "I study Cryptography" with depth 2 and 3 separately using Rail Fence Cipher.

⇒ Here: Key: Rail fence of depth 2

plaintext: I study Cryptography

Now, the ciphertext is produced by transcribing the first row followed by the second row on two lines in a zig-zag pattern.

I		T		D		C		Y		T		G		A		H	
	S		U		Y		R		P		O		R		P		Y

Ciphertext: IIDCYTGAHSUYRPORPY

Again, Key: Rail fence of depth 3

plaintext: Istudy Cryptography

Writing plaintext on three lines in a zig-zag pattern.

I			D			Y			G			H	
	S		U		Y		R		P		O		R		P		Y
		T				C			T			A					

Ciphertext: IDYGHSUYRPORPYTCTA

(16) What is One time pad Cipher? Explain with example.

One time pad cipher is an unbreakable cyptosystem. It is an encryption technique that uses a random key that is as long as the message being encrypted. The key is used only once and then discarded which ensures perfect secrecy.

The system can be expressed as follows:

$C_i = P_i \oplus K_i$

$P_i = C_i \oplus K_i$ where, C_i = i^{th} binary ~~bit~~ digit of Cipher text

P_i = i^{th} binary ~~bit~~ digit of plain text

K_i = i^{th} binary ~~bit~~ digit of key

$\oplus$ = Exclusive OR operation.

Example: plaintext = 00101001
key = 10101100

Ciphertext = 10000101

(17) What is Hill Cipher? Encrypt the message 'paymoremoney' with key given below: $\begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 9 \end{bmatrix}$

⇒ Hill Cipher is a classical symmetric-key encryption algorithm that uses linear algebra concepts, specifically matrix multiplication, to encrypt and decrypt text. It is one of the earliest polygraphic ciphers, meaning it encrypts multiple letters at once.

Next part:

Since the key is 3x3 Matrix, plaintext should be converte into vectors of length 3. So, $\begin{bmatrix} p \\ a \\ y \end{bmatrix}_{3\times1}$ $\begin{bmatrix} M \\ O \\ R \end{bmatrix}_{3\times1}$ $\begin{bmatrix} E \\ M \\ O \end{bmatrix}_{3\times1}$ $\begin{bmatrix} N \\ E \\ Y \end{bmatrix}_{3\times1}$

(1) 1st vector: $\begin{bmatrix} p \\ a \\ y \end{bmatrix} = \begin{bmatrix} 15 \\ 0 \\ 24 \end{bmatrix}$, key = $\begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 9 \end{bmatrix}$

$C = KP \bmod 26$

$= \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 9 \end{bmatrix} \begin{bmatrix} 15 \\ 0 \\ 24 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 375 \\ 819 \\ 246 \end{bmatrix} \bmod 26 = \begin{bmatrix} 11 \\ 13 \\ 12 \end{bmatrix} = \begin{bmatrix} L \\ N \\ M \end{bmatrix}$

② 2nd vector: $\begin{bmatrix} M \\ O \\ R \end{bmatrix} = \begin{bmatrix} 12 \\ 14 \\ 17 \end{bmatrix}$

$C = KP \bmod 26 = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 9 \end{bmatrix} \begin{bmatrix} 12 \\ 14 \\ 17 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 527 \\ 861 \\ 205 \end{bmatrix} \bmod 26 = \begin{bmatrix} 7 \\ 3 \\ 23 \end{bmatrix}$

Here, $\begin{bmatrix} 7 \\ 3 \\ 23 \end{bmatrix} = \begin{bmatrix} H \\ D \\ X \end{bmatrix}$

③ 3rd vector: $\begin{bmatrix} E \\ M \\ O \end{bmatrix} = \begin{bmatrix} 4 \\ 12 \\ 14 \end{bmatrix}$

$C = KP \bmod 26 = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 9 \end{bmatrix} \begin{bmatrix} 4 \\ 12 \\ 14 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 342 \\ 594 \\ 158 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 4 \\ 22 \\ 2 \end{bmatrix} = \begin{bmatrix} E \\ W \\ C \end{bmatrix}$

④ 4th vector: $\begin{bmatrix} N \\ E \\ Y \end{bmatrix} = \begin{bmatrix} 13 \\ 4 \\ 24 \end{bmatrix}$

$C = KP \bmod 26 = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 9 \end{bmatrix} \bmod 26 \times \begin{bmatrix} 13 \\ 4 \\ 24 \end{bmatrix} \bmod 26$

$$= \begin{bmatrix} 409 \\ 849 \\ 250 \end{bmatrix} \bmod 26 = \begin{bmatrix} 19 \\ 17 \\ 16 \end{bmatrix} = \begin{bmatrix} T \\ R \\ Q \end{bmatrix}$$

∴ Ciphertext: "LNMHDXEWCTRQ"

$$= \begin{bmatrix} 409 \\ 849 \\ 250 \end{bmatrix} \bmod 26 = \begin{bmatrix} 19 \\ 17 \\ 16 \end{bmatrix} = \begin{bmatrix} T \\ R \\ Q \end{bmatrix}$$

∴ Ciphertext: "LNMHDXEWCTRQ"

Assignment 2

① Find the GCD of 2740 and 1760, using Euclidean algorithm.

⇒ The Euclidean algorithm states that:

$$\gcd(a,b) = \gcd(b, a \bmod b)$$

Using Euclidean algorithm,

2740 = 1x1760 + 980	gcd(1760, 980)
1760 = 1x980 + 780	gcd(980, 780)
980 = 1x780 + 200	gcd(780, 200)
780 = 3x200 + 180	gcd(200, 180)
200 = 1x180 + 20	gcd(180, 20)
180 = 9x20 + 0	gcd(20, 0)

Since, the remainder is 0, the divisor 20 is the GCD.

∴ gcd(2740, 1760) = 20

② Find the gcd of 42823 and 6409

Using Euclidean Algorithm,

42823 = 6x6409 + 4369

6409 = 1x4369 + 2040

4369 = 2x2040 + 289

2040 = 7x289 + 17

289 = 17x17 + 0

Since, the remainder is 0, gcd(42823, 6409) = 17

③ Find the multiplicative inverse of
@ $50^{b} \bmod 71^{m}$

⇒

Q	A1	A2	A3	B1	B2	B3	T1	T2	T3
1	1	0	71	0	1	50	1	-1	21
*2	0	1	50	1	-1	21	-2	3	8
2	1	-1	21	-2	3	8	5	-7	5
1	-2	3	8	5	-7	5	-7	10	0
	5	-7	5	-7	10	0			

Since, B3 = 0 , no inverse exists.

⇒

A1	A2	A3	B1	B2	B3	Q	T1	T2	T3
1	0	71	0	1	50	1	1	-1	21
0	1	50	1	-1	21	2	-2	3	8
1	-1	21	-2	3	8	2	5	-7	5
-2	3	8	5	-7	5	1	-7	10	3
5	-7	5	-7	10	3	1	12	-17	2
-7	10	3	12	-17	2	1	-19	27	1
12	-17	2	-19	27	1				

Since, B3 = 1 , $B2 = b^{-1} \bmod m$

i.e. ~~-19~~ 27

~~Finding the positive multiplicative inverse,~~

~~$-19 \bmod 71 = 52$~~

Thus, the multiplicative inverse of 50 mod 71 is 827.

(b) 43 mod 64

⇒

A1	A2	A3	B1	B2	B3	Q	T1	T2	T3
1	0	64	0	1	43	1	1	-1	21
0	1	43	1	-1	21	2	-2	3	1
1	-1	21	-2	3	1				

Since, $B3 = 1$, $B2 = b^{-1} \bmod m$

i.e. 3

Thus, the multiplicative inverse of 43 mod 64 is 3.

(c) Find the modular multiplicative inverse of 11 in $\mathbb{Z}_{26}$.

⇒ To find the modular multiplicative inverse of 11 in $\mathbb{Z}_{26}$, we need to find an integer x such that:

$$11x \equiv 1 \pmod{26}$$

By hit and trial method,

substitute x as 19 we get,

$$11 \times 19 \equiv 1 \pmod{26}$$

Check: $11 \times 19 = 209$

$209 \bmod 26 = 1$

Hence, the modular multiplicative inverse of 11 in $\mathbb{Z}_{26}$ is 19.

Ans

(d) Define finite fields of Order p.

For a given prime, p, the finite field of order p, GF(p) is defined as the set $\mathbb{Z}_p$ of integers $\{0, 1, \ldots, p-1\}$, together with the arithmetic operations modulo p. (GF stands for Galois field. Arithmetic in GF(q)

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

(a) Addition Modulo 4.

×	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

(b) Multiplicative modulo 4.

⑤ Define the term irreducible polynomial and write the irreducible polynomial used by AES in GF(8).

⇒ An irreducible polynomial over a given field is a polynomial that cannot be factored into the product of two non-constant polynomials within that field. In other words, it has no divisors other than itself and 1 (up to multiplication by field elements).

AES operates over the Galois field $GF(2^8)$. The irreducible polynomial used for constructing this field is:

$$p(x) = x^8 + x^4 + x^3 + x + 1$$

This polynomial is used in AES to perform modular reduction when performing finite field arithmetic.

⑥ Find the arithmetic multiplication in $GF(2^8)$ for the following:

ⓐ $\{02\} \cdot \{87\} \bmod \{11B\}$

Solution:

Converting Hex to Binary

$\{02\} = 00000010$

$\{87\} = 10000111$

Representing as polynomials:

$\{02\} = x$

$\{87\} = x^7 + x^2 + x + 1$

Now, Multiplying the polynomials,

$$x \cdot (x^7 + x^2 + x + 1) = x^8 + x^3 + x^2 + x$$

Here, The polynomial $\{11B\}$ corresponds to $x^8 + x^4 + x^3 + x + 1$

Then,

$x^8 + x^3 + x^2 + x \bmod x^8 + x^4 + x^3 + x + 1$ is calculated as:

$x^8 \overline{)} x^4 +$

$$x^8+x^4+x^3+x^2+1 \;\overline{)}\; x^8+x^3+x^2+x \;(\;1$$
$$\underline{x^8+x^4+x^3+x+1}$$
$$x^4+x^2+1$$

$\therefore x^8+x^3+x^2+x \bmod x^8+x^4+x^3+x+1$ is x^4+x^2+1

Again, Converting the result back to Hexadecimal:

$x^4+x^2+1 = 00010101$

$\underline{0001}\,\underline{0101} = 15_{16}$

Hence,

The arithmetic multiplication of $\{02\} \cdot \{87\}$ in GF(2^8) modulo $\{11B\}$ is:

$\{02\} \cdot \{87\} = \{15\}$

Note:

Conversion to polynomial:

11B ⇒ first convert to binary

$\underset{x^8\;x^4\;x^3\;x^2\;x^1}{\underline{0001}\,\underline{0001}\,\underline{1011}}$

Then, place the bitposition on the power of x wherever it is 1.

i.e. $x^9+x^5+x^4+x+1$

⑥ Compute $x^{12}+x^9+x^7+x^5+x^2$ mod $x^8+x^4+x^3+x+1$

⇒ Here, we perform polynomial division where addition is XOR.

$$
\begin{array}{r}
x^4+x+1 \\
x^8+x^4+x^3+x+1 \overline{)\,x^{12}+x^9+x^7+x^5+x^2} \\
\underline{x^{12}+x^8+x^7+x^5+x^4} \\
x^9+x^8+x^4+x^2 \\
\underline{x^9+x^5+x^4+x^2+x} \\
x^8+x^5+x \\
\underline{x^8+x^4+x^3+x+1} \\
x^5+x^4+x^3+1
\end{array}
$$

Hence, the result is : $x^5+x^4+x^3+1$

⑦ For given $f(x)=x^3+x^2$ and $g(x)=x^9+x+1$. find $f(x)+g(x)$, $f(x) \times g(x)$ in GF(8)

⇒ Here,

⊙ $f(x)\cdot g(x)$ is standard polynomial multiplication

⊙ $f(x)*g(x)$ involves polynomial multiplication followed by reduction modulo an irreducible polynomial of degree 3 (since $GF(8)=GF(2^3)$).

Given:

$f(x)=x^3+x^2$

$g(x)=x^2+x+1$ (assuming $g(x)=x^2+x+1$ for GF(8) as x^9+x+1 is not valid in GF(8))

Then,

$$
\begin{aligned}
f(x)\cdot g(x) &= (x^3+x^2)(x^2+x+1) \\
&= x^5+x^4+x^3+x^4+x^3+x^2 \\
&= x^5+x^2
\end{aligned}
$$

$f(x) * g(x)$ in GF(8)

In GF(8), arithmetic is performed modulo an irreducible polynomial of degree 3. A common choice for GF(8) is

$$p(x) = x^3 + x + 1$$

So, $f(x) * g(x)$ becomes: $f(x) \cdot g(x) \bmod p(x)$

or, $x^5 + x^2 \bmod x^3 + x + 1$

$$x^3+x+1 \overline{)\, x^5+x^2 \,(x^2+1}$$

$$\underline{x^5+x^3+x^2}$$

$$x^3$$

$$\underline{x^3+x+1}$$

$$x+1$$

$\therefore f(x) * g(x) = x+1$

(3) Find the GCD of x^2+7x+6 and x^2-5x+6 using Euclidean algorithm.

⇒ Solution:

Q	A	B	R
1	x^2+7x+6	x^2-5x-6	$12x+12$
$x/12$	x^2-5x-6	$12x+12$	$-6x-6$
-2	$12x+12$	$-6x-6$	0
	$-6x-6$	0	

$\therefore$ GCD $= -6x-6$ (Dividing to make leading coefficient 1), we get,

GCD $= x+1$

Ans

Rough:

$$x^2-5x-6 \overline{)\, x^2+7x+6 \,(1}$$

$$\underline{x^2-5x-6}$$

$$12x+12$$

$$12x+12 \overline{)\, x^2-5x-6 \,(\frac{x}{12}}$$

$$\underline{x^2+x}$$

$$-6x-6$$

$$-6x-6 \overline{)\, 12x+12 \,(-2}$$

$$\underline{12x+12}$$

$$0$$

(9) Encrypt plaintext 'ABRA KA DABRA' with Caesar cipher with key = 8 and Rail fence cipher with rails = 3.

⇒ Solution:

Plaintext = 'abra ka dabra'

(i) Caesar Cipher with key = 8

Here, we shift each letter forward by 8 positions and if the shift goes past 'z', it wraps around to the beginning of the alphabet:

Hence, Ciphertext = ijzi si' Lijzi

(ii) Rail fence cipher with rails = 3

a				k				b						
	b		a		a		a		r					
		r				d				a				

Ciphertext = akbbaaarrda

(10) What is Hill Cipher? Encrypt the message 'paymoremoney' with key below:

$$\begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 9 \end{bmatrix}$$

⇒ look Assignment 1.

(11) Encrypt the text 'welcometocryptoclass' using the key 'diamond' with playfair cipher and decrypt the resulting cipher.

⇒ Given:

plaintext = 'welcometocryptoclass'

key = 'diamond'

Creating 5x5 playfair Matrix

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

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

Creating 5x5 playfair Matrix:

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

Encrypting using playfair cipher:

we ⇉ YB, lc ⇉ KE, om ⇉ DO, et ⇉ LY, OC ⇉ AF, RY ⇉ TW,
PT ⇉ LU, OC ⇉ AF, LA ⇉ KM, SX ⇉ XA, SX ⇉ XA

∴ Ciphertext = YBKEDOLYAFTWLUAFKMXAXA

Decrypting the cipher text:

YB ⇉ WE, KE ⇉ LC, DO ⇉ OM, LY ⇉ ET, AF ⇉ OC, TW ⇉ RY,
LU ⇉ TP, AF ⇉ OC, KM ⇉ LA, XA ⇉ SX, XA ⇉ SX

Decrypted plaintext = Welcometocryptoclasxsx

Remove the filler "x" letters:

plaintext = welcometocryptoclass

(12) For given 3rd round key as A2 D4 FA 22 45 65 70 89 02 47 EA F4 64 11 44 B8, find the 4th Round key. Use necessary data structures of AES.

⇒ Solution:

Given, 3rd Round key consists of words w[12-15] and 4th round key consists of words w[16-19].

So, To find the 4th Round key, we find w[16-19].

Now, $w_i = w_{16}$ i.e. is multiple of 4

Temp = w[i-1] = w_{15} = 64 11 44 B8

After Rotate Word, 11 44 B8 64

After Sub Word, 82 1B 6C 43

RCON(j) = RCON(i/4) = RCON(16/4) = RCON(4)

= (08 00 00 00)

After XOR with Rcon i.e. XOR 82 1B 6C 43 with 08 00 00 00.

(sub(rotate(word) + RCON(i/4))

8A 1B 6C 43 which is g or t or temp.

$w[i] = g \oplus w[i-4]$

or, w_{16} = 8A 1B 6C 43 ⊕ A2 D4 FA 22

= 28 CF 96 61

$w_{17} = w_{16} \oplus w_{13}$

= 28 CF 96 61 ⊕ 45 65 70 89

= 6D AA E6 E8

$w_{18} = w_{17} \oplus w_{14}$ = 6D AA E6 E8 ⊕ 02 47 EA F4

= 6F ED 0C 1C

$w_{19} = w_{18} \oplus w_{15}$ = 6F ED 0C 1C ⊕ 64 11 44 B8

= 0B FC 48 AF

Hence, 4th Round key is [28 CF 96 61 6D AA E6 E8 6F ED 0C 1C 0B FC 48 AF]

Ans

(19) Find the Euler's totient function of 24.

⇒ Euler's totient function $\phi(n)$ is defined as the number of positive integers less than n and relatively prime to n.

Euler's Totient function $\phi(n)$ counts the number of integers from 1 to n that are coprime to n. For $n = 24$, the numbers coprime to 24 are:

1, 5, 7, 11, 13, 17, 19, 23

$\therefore \phi(24) = 8$

Ans

(13) Find the Euler's totient function of 24.

⇒ Euler's totient function $\phi(n)$ is defined as the number of positive integers less than n and relatively prime to n.

Euler's Totient function $\phi(n)$ counts the number of integers from 1 to n that are coprime to n. For $n = 24$, the numbers coprime to 24 are:

1, 5, 7, 11, 13, 17, 19, 23

$\therefore \phi(24) = 8$

Ans

Assignment: 3

(1) Check Whether 5 is primitive root of 23 or not. Justify with the reasons.

⇒ We know that, 'α' is said to be primitive root of prime number 'p' if $\alpha^1 \bmod p$, $\alpha^2 \bmod p$, $\alpha^3 \bmod p$ --- $\alpha^{p-1} \bmod p$ are distinct.

The primitive root condition requires that the order of 5 must be equal to $\phi(23)$, where $\phi(23) = 23 - 1 = 22$.

Thus we check $5^d \bmod 23$ for divisors of 22: 1, 2, 11, 22.

Now, Computing powers of 5 mod 23

1) $5^1 \bmod 23 = 5$

2) $5^2 \bmod 23 = 25 \bmod 23 = 2$

3) $5^{11} \bmod 23 = (5^2)^5 \times 5 \bmod 23$

We know, $5^2 \bmod 23 = 2$

$5^4 \bmod 23 = 2^2 \bmod 23 = 4$

$5^8 \bmod 23 = (5^4)^2 \bmod 23 = 16 \bmod 23 = 16$

$5^{10} \bmod 23 = (5^8 \times 5^2) \bmod 23 = 16 \times 2 \bmod 23$

$= 32 \bmod 23$

$= 9$

$\therefore 5^{11} \bmod 23 = (5^{10} \times 5) \bmod 23 = 9 \times 5 \bmod 23 = 45 \bmod 23$
$= 22$

Since, $22 \equiv -1 \pmod{23}$, we get

④ $5^{22} \bmod 23 = (5^{11})^2 \bmod 23 = 1$

Conclusion: ⊙ The smallest exponent for which $5^d \equiv 1 \pmod{23}$ is $d = 22$.

⊙ Since the order of 5 is exactly $\phi(23) = 22$, 5 is a primitive root of 23.

Thus, 5 is a primitive root of 23 because it has order 22, meaning it generates all residues modulo 23.

② Encrypt the text '2' using RSA algorithm with $p = 3$ $q = 11$ and also decrypt the resulting cipher.

⇒ Solution:

Given: $p = 3$, $q = 11$

Then, $n = p \times q = 3 \times 11 = 33$

$\phi(n) = (p-1) \times (q-1) = (3-1) \times (11-1) = 2 \times 10 = 20$

Now, we choose public key e such that:

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

let's choose $e = 3$. Verify that $\gcd(3, 20) = 1$. This is valid.

Then, we compute private key d such that:

$ed \equiv 1 \pmod{\phi(n)}$ or, $d \equiv e^{-1} \pmod{\phi(n)}$

i.e. $3 \cdot d \equiv 1 \pmod{20}$

Taking $d = 7$, $21 \equiv 1 \pmod{20}$. This is valid

Now, Encrypting the plaintext:

$C = m^e \pmod{n}$

Here, $m = 2$, $e = 3$ and $n = 33$

$C = 2^3 \pmod{33} = 8$

∴ The ciphertext is 8.

Then, decrypting the ciphertext:

$$m = c^d \pmod n$$

Here, $c = 8$, $d = 7$ and $n = 33$

$$m = 8^7 \pmod{33} = 2$$

∴ The decrypted plaintext is 2.

③ Answer of Q.No.3

To solve this problem, we need to use Alice's public and private keys to encrypt the message $M = 13$ into ciphertext C and then recover the message R using Alice's private key. We'll assume Alice's RSA keys are generated as follows:

Let, $p = 3$, $q = 11$

Then, $n = p \times q = 3 \times 11 = 33$

$$\phi(n) = (p-1)(q-1) = (3-1) \times (11-1) = 20$$

Choose $e = 3$; check $\gcd(e, \phi(n)) = 1$

Compute d such that $ed \equiv 1 \pmod{\phi(n)}$

By testing, we get $d = 7$.

Now, Using Alice's public key $(e,n) = (3,33)$, the ciphertext C is computed as: $C \equiv M^e \pmod n$

$$C = 13^3 \pmod{33}$$

$$C = 19$$

Using Alice's private key $(d,n) = (7,33)$, the recovered message R is computed as: $R \equiv c^d \pmod n$

$$R \equiv 19^7 \pmod{33}$$

$$R = 13$$

Final ~~Ans~~ Answer: Ciphertext $C = 19$

Recovered Message $R = 13$

Answer of Q.No.4

Solution:

Here, $p = 23$ and $q = 19$

$e = 283$ and $n = pq = 23 \times 19 = 437$

We know that, $ed \equiv 1 \pmod{\phi(n)}$

$\phi(n) = (p-1)(q-1) = 396$

Then,

$283 \times d \equiv 1 \pmod{396}$

Using Extented Euclidean Algorithm

$396 = 283 \cdot 1 + 113$

~~$283 = 113 \cdot 1 + 170$~~

$283 = 113 \cdot 2 + 57$

$113 = 57 \cdot 1 + 56$

$57 = 56 \cdot 1 + 1$

$56 = 1 \cdot 56 + 0$

Back-substitute:

$1 = 57 - 1 \cdot 56$

$1 = 113 - 1 \cdot 57 - 1 \cdot (113 - 1 \cdot 57)$

$1 = 2 \cdot 57 - 113$

$1 = 2 \cdot (283 - 2 \cdot 113) - 113$

$1 = 2 \cdot 283 - 5 \cdot 113$

$1 = 2 \cdot 283 - 5(396 - 1 \cdot 283)$

$1 = 7 \cdot 283 - 5 \cdot 396$

Thus, $d = 7$

Hence, Dexter public key is $(e, n) = (283, 437)$

Dexter private key is $(d, n) = (7, 437)$

Answer of Q.No.5

Solution:

Given: $p = 11$, $g = 2$, $x_A = 9$, $x_B = 4$

Here, x_A and x_B are secret keys.

Now, A computes its public key Y_A as:

$$Y_A = g^{x_A} \pmod p$$

$$\text{or, } Y_A = 2^9 \pmod{11}$$

$$\text{or, } Y_A = 6$$

Similarly, B computes its public key Y_B as:

$$Y_B = g^{x_B} \pmod p$$

$$\text{or, } Y_B = 2^4 \pmod{11}$$

$$\text{or, } Y_B = 5$$

Then, the session key K is computed by both A and B using each other's public keys.

A computes K as: $K = (Y_B)^{x_A} \pmod p$

$$= 5^9 \pmod{11}$$

$$= 9$$

B computes K as: $K = (Y_A)^{x_B} \pmod p$

$$= 6^4 \pmod{11}$$

$$= 9$$

Hence, the session key is 9. Ans

Answer of Q.No.6

Solution:

Here, $p = 7$, $g = 3$, $x_A = 2$, $x_B = 5$

Then, $Y_A = g^{x_A} \pmod p = 3^2 \pmod 7 = 2$

$Y_B = g^{x_B} \pmod p = 3^5 \pmod 7 = 5$

Their common session key $(K) = (Y_B)^{x_A} \pmod p = 5^2 \pmod p$

$= 4$

Hence, their common session key is 4.

Answer of Q.No.7

Solution:

prime value (q) = 17

primitive root (g) = 5

Alice's secret key (X_A) = 4

Bob's secret key (X_B) = 6

Now, Alice's public key $(Y_A) = g^{X_A} \pmod q$

$= 5^4 \pmod{17}$

$= 13$

Bob's public key $(Y_B) = g^{X_B} \pmod q$

$= 5^6 \pmod{17}$

$= 2$

Then, Session key $(K) = (Y_B)^{X_A} \pmod q$ Or, $(Y_A)^{X_B} \pmod q$

$= 2^4 \pmod{17}$

$= 16$

Hence, the secret key they exchanged is 16.

Answer of Q.No.8

Solution:

$q = p = 467$ (prime)

$g = 2$ (primitive root modulo p)

$a = 153$ (Alice's private key)

Now, Alice's public key A is computed as:

$A \equiv g^a \pmod p$

Or, $A \equiv 2^{153} \pmod{467}$

Or, $A = 224$

Hence, Alice's public key is $(p, g, A) = (467, 2, 224)$

Bob wants to send the message $m = 331$ to Alice. He chooses an ephemeral key $k = 197$. The ciphertext (c_1, c_2) is

① $c_1 \equiv g^k \pmod p$

or, $c_1 \equiv 2^{197} \pmod{467}$

or, $c_1 = 87$

② $c_2 \equiv m \cdot A^k \pmod p$

or, $c_2 = 331 \cdot 224^{197} \pmod{467}$

or, $c_2 = 57$

Hence, the ciphertext pair is : $(87, 57)$

Alice decrypts the ciphertext (c_1, c_2) using her private key $a = 153$. The decrypted message m is computed as;

$$m \equiv c_2 \cdot (c_1^a)^{-1} \pmod p$$

First, compute $c_1^a \pmod p$

$$c_1^a \equiv 87^{153} \bmod 467$$

$$\Rightarrow c_1^a = 367$$

Now, compute the modular inverse of 367 modulo 467

$$367^{-1} \pmod{467} = 14$$

Then, compute the decrypted message m:

$$m \equiv c_2 \cdot (c_1^a)^{-1} \pmod p$$

$$m \equiv 57 \cdot 14 \pmod{467}$$

$$57 \cdot 14 = 798 = 798 - 1 \cdot 467 = 331 \pmod{467}$$

Hence, the decrypted message m is 331

Ans