Q.1 Explain additive cipher? use additive cipher with key 2 to encrypt message "DEPARTMENT".

→

| A | B | C | D | E | F | G | H | I | J |
|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |

| K | L | M | N | O | P | Q | R | S | T |
|---|---|---|---|---|---|---|---|---|---|
| 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 |

| U | V | W | X | Y | Z |
|---|---|---|---|---|---|
| 20 | 21 | 22 | 23 | 24 | 25 |

| plaintext = | D | E | P | A | R | T | M | E | N | T |
|---|---|---|---|---|---|---|---|---|---|---|
| | 3 | 4 | 15 | 0 | 17 | 19 | 12 | 4 | 13 | 19 |

key = 2

Encryption using additive cipher :→

Ciphertext = (plaintext + key) mod 26

① C = (P+K) mod 26
= (D+K) mod 26
= (3+2) mod 26
= 5 mod 26
= 5 ∼ F

② C = (E+K) mod 26
= (4+2) mod 26
= 6 mod 26
= 6 ∼ G

③ C = (P+K) mod 26
= (15+2) mod 26
= 17 mod 26
= 17 ∼ R

④ C = (A+K) mod 26
= (0+2) mod 26
= 2 mod 26
= 2 ∼ C

Teacher's Signature

⑤ $C = (R+K) \bmod 26$
$= (17+2) \bmod 26$
$= 19 \bmod 26$
$= 19 \sim T$

⑦ $C = (M+K) \bmod 26$
$= (12+2) \bmod 26$
$= 14 \bmod 26$
$= 14$
$= O$

⑥ $C = (T+K) \bmod 26$
$= (19+2) \bmod 26$
$= 21 \bmod 26$
$= 21 \sim V$

⑧ $C = (N+K) \bmod 26$
$= (13+2) \bmod 26$
$= 15 \bmod 26$
$= 15 \sim P$

∴ Cipher Text = FIGRCTVOGPV.

* Additive cipher :-

① An additive cipher is a type of mono-alphabetic cipher that shifts the plaintext alphabets by a fixed amount to obtain the cipher alphabet.

② It is also refered as 'shift cipher' or 'caesar cipher'

③ As name suggests, addition modulus 2 operation is performed on plain text to obtain a cipher text.

④ $C = (P+K) \bmod 26$
$P = (C+K) \bmod 26$
where,

Teacher's Signature

P = plaintext / message

C = ciphertext

k = key

(5) It is not very secure. It can be broken by brute force attacks.

(6) It means the message encrypted by this method can easily decrypted.

(7) It is the weak method of cryptography.

(8) Advantages :→

1) Very easy to implement

2) Simplest method and only one key is used in its entire process.

3) It requires only few computing resources.

(9) Disadvantages :→

1) It can be easily hacked

2) It provide very little security

3) By looking at the pattern of letter in it, the entire message can decrypted easily.

Question 2. Explain Substitution techniques ? Using the key "COMPUTER" encrypt the message "TRANSFER" by using Vigenere cipher.

→ * Substitution technique :→

(1) Substitution technique is a classical encryption technique where the characters present in the original message are replaced by other characters or numbers or by symbols.

(2) If the plain text is considered as the string of bits, then the substitution technique would replace bit pattern of plain text with the bit pattern of cipher text.

(3) Some substitution techniques are

a) Caesar Cipher.

b) Monoalphabetic Cipher

c) polyalphabetic cipher.

d) playfair cipher

e) Hill Cipher

f) one-Time pad.

*

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Key = | C | O | M | P | U | T | E | R |
| | 2 | 14 | 12 | 15 | 20 | 19 | 4 | 17 |
| plaintext = | T | R | A | N | S | F | E | R |
| | 14 | 17 | 0 | 13 | 18 | 5 | 4 | 17 |

Teacher's Signature

Encryption :

① $C = (P+K) \bmod 26$
$= (2+19) \bmod 26$
$= 21 \bmod 26$
$= 21 \sim V$

② $C = (P+K) \bmod 26$
$= (14+17) \bmod 26$
$= 31 \bmod 26$
$= 5 \sim F$

③ $C = (P+K) \bmod 26$
$= 12 \bmod 26$
$= 12 \sim M$

④ $C = (P+K) \bmod 26$
$= (15+13) \bmod 26$
$= 28 \bmod 26$
$= 2 \sim C$

⑤ $C = (P+K) \bmod 26$
$= (20+18) \bmod 26$
$= 38 \bmod 26$
$= 12 \sim M$

⑥ $C = (P+K) \bmod 26$
$= (19+5) \bmod 26$
$= 24 \bmod 26$
$= 24 \sim Y$

⑦ $C = (P+K) \bmod 26$
$= 8 \bmod 26$
$= 8 \sim I$

⑧ $C = (P+K) \bmod 26$
$= (17+17) \bmod 26$
$= 34 \bmod 26$
$= 8 \sim I$

∴ Ciphertext = VFMCMYII

Teacher's Signature

Decryption :

① $P = (C - K) \bmod 26$
$= (21 - 2) \bmod 26$
$= 19 \bmod 26$
$= 19 \sim T$

② $P = (5 - 14) \bmod 26$
$= 17 \sim R$

③ $P = (12 - 12) \bmod 26$
$= 0 \bmod 26$
$= 0 \sim A$

④ $P = (2 - 15) \bmod 26$
$= 13 \sim N$

⑤ $P = (12 - 20) \bmod 26$
$= 18 \sim S$

⑥ $P = (24 - 19) \bmod 26$
$= 5 \bmod 26$
$= 5 \sim F$

⑦ $P = (8 - 4) \bmod 26$
$= 4 \bmod 26$
$= 4 \sim E$

⑧ $P = (8 - 17) \bmod 26$
$= 17 \sim R$

$\therefore$ plaintext = TRANSFER.

Teacher's Signature

Question 3. Explain the Substitution Techniques ? if the cipher is keyed by a word "COMPUTER" and plaintext is "please transfer one million dollars to my account Six Six two obtain the cipher text by playfair substitution methods ?

→

* Substitution Techniques :→

(1) A Substitution cipher simply means that each letters in the plaintext is substituted with another letter to form the ciphertext.

(2) Substitution technique is a classical encryption approach where the characters present in the initial message are restored by the other characters or number or by symbol.

(3) There are various types of substitution ciphers;
   a) monoalphabetic cipher.
   b) polyalphabetic cipher.

plaintext = PLEASE TRANSFER ONE MILLION DOLLARS TO MY ACCOUNT SIX SIX TWO.

Key = COMPUTER

Teacher's Signature

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

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| PL | EA | SE | TR | AN | SF | ER | OM | EM | IL | LI |
| OΦ | RB | LB | EA | RΦ | LI | RA | ML | RO | FS | SF |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| ON | DO | LX | EA | RS | TO | MY | AC | CO | UN | TS |
| ML | FC | NW | ΦE | BM | EC | PX | TP | OM | MS | BK |

| | | | |
|---|---|---|---|
| IX | SI | XT | WO |
| GZ | ZI | VR | OE |

Ciphertext : OΦRBLB EARΦLIRA MLR OFSSFML FCNWΦEBM EC PX TPOMMSBK KGZ ZIV ROE

Q.4 One time pad :

plaintext = SUBJECT

key = abcd

⇒

plaintext = SUBJECT

key = abcdefg

adding e f g, because length of plaintext & key must be same in one time pad

| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |

| Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|
| 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

plain text = S U B J E C T

18 20 1 9 4 2 19

key = a b c d e f g

0 1 2 3 4 5 6

Add: 18 21 3 12 8 7 25

(plaintext + key)

Subtract: 18 21 3 12 8 7 25

(Subtract if no. is greater than 26)

Cipher text = S V D M I H Z

18 21 3 12 8 7 25

Teacher's Signature

Ques.5) Explain DES in detail.

→ (1) DES stands for Data Encryption Standard.

(2) The DES algorithm was a key of 56 bit size.

(3) Using the key, the DES takes a block of 64 bit plain text as input and generates a block of 64 bit cipher text.

(4) General structure of DES is depicted in the following illustration:

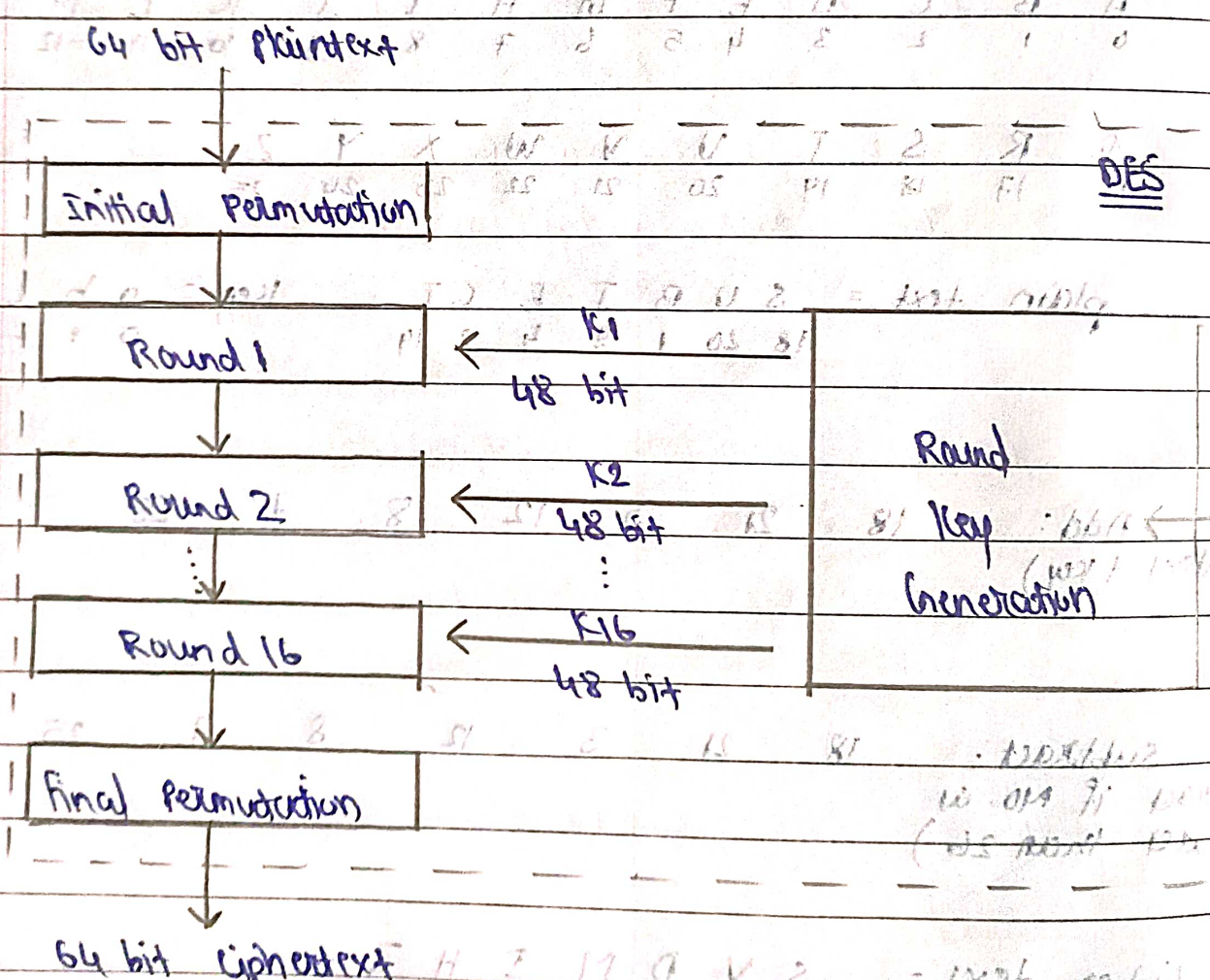



Fig: DES

Teacher's Signature

(5) DES is an implementation of Feistel cipher. It uses 16 round Feistel structure.

(6) Since DES is based on the Feistel cipher, all that is required to specify DES is -

- Round function
- Key Schedule
- Any additional processing - initial and final permutation

(7) The encryptor and the decryptor need to use the same key otherwise they will not be able to communicate together.

(8) The decryption process is the exact opposite of the encryption. It takes in a 64 bit block of ciphertext and produces the 64-bit block of plaintext using the same 48 bit key during encryption.

Teacher's Signature _____

Q.6 Difference between :→

a) Private Vs Public key cryptography
b) Conventional Vs public key encryption
c) Symmetric Vs Asymmetric cryptography.

→

| Private key Cryptography | Public key cryptography |
|---|---|
| (1) Private key is faster than the public key | (1) It is slower than private key. |
| (2) In this, the same key & algo. are used to encrypt and decrypt the message | (2) In this, two keys are used. |
| (3) private key is symmetrical because there is only one key that is called Secrete key | (3) public key is asymmetrical because there are two keys. |
| (4) It is efficient technology | (4) It is an inefficient technology. |
| (5) It is used for large amount of text | (5) It is used for only short message. |

Teacher's Signature

Q.7 Explain a AES algorithm ? How is different from DES algorithm ? in details.

→ AES algorithm :→

① AES : Advance Encryption Standard.

② AES is block cipher , encrypts data in blocks of 128 bit each.

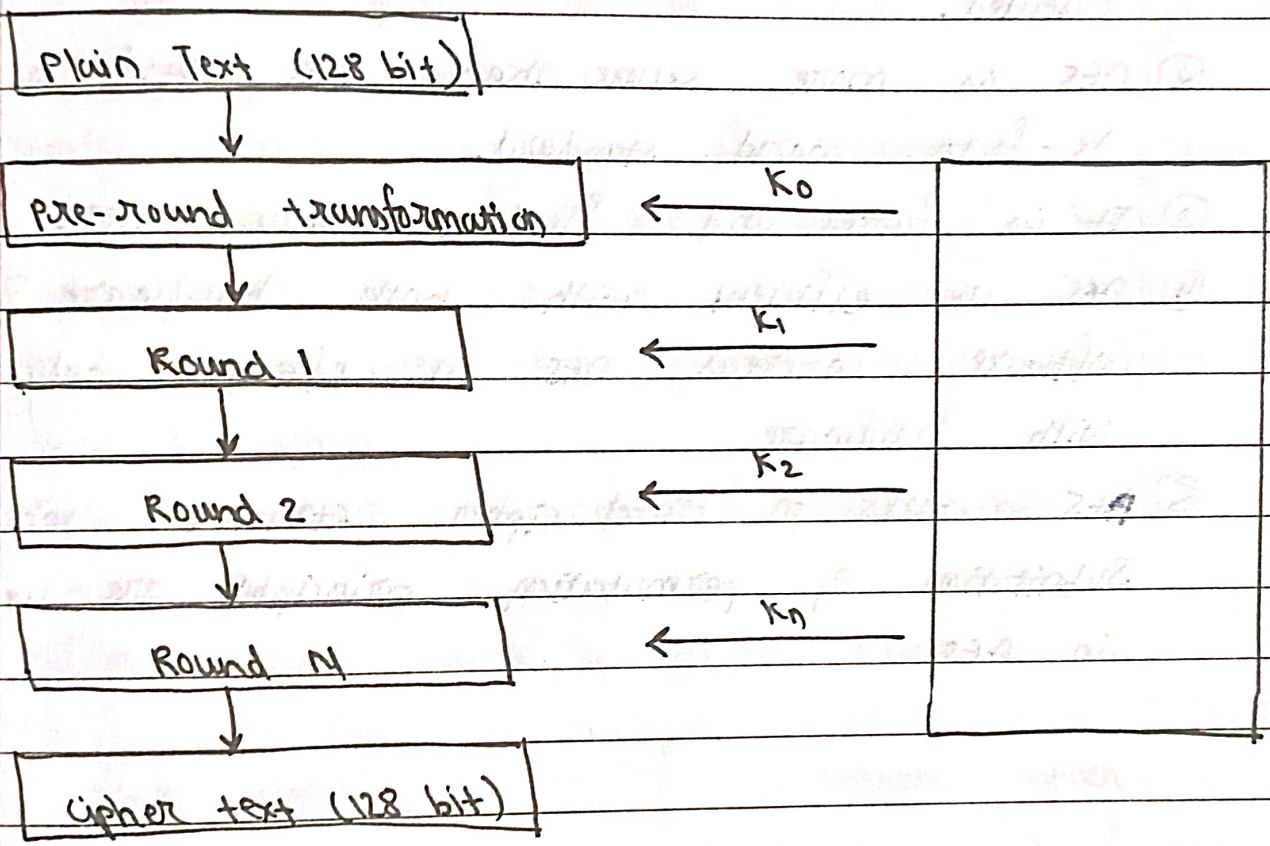



Fig : Creation of Round keys.

③ It converts individual block using key of 128, 192 & 256 bits.

④ Once it encrypts these blocks , it joints them together to form the ciphertext.

Teacher's Signature

(5) AES implemented in s/w and h/w throughout the world to encrypt sensitive data.

* AES and DES comparison:

(1) AES is byte oriented whereas DES is bit oriented.

(2) AES is more secure than DES and is the de-facto world standard.

(3) It is faster and flexible than DES.

(4) AES is efficient with both hardware & Software whereas DES is efficient only with hardware.

(5) DES works on Feistel cipher structure whereas Substitution & permutation principles are used in AES

Teacher's Signature

Q.8 Explain a block cipher principle ? what is difference between stream cipher and block cipher ?

→ * Block cipher :→

① Block ciphers are built in the Feistal cipher structure.

② It has a specific no. of rounds and keys for generating ciphertext.

③ Block cipher is a type of encryption algorithm that processes fixed-size blocks of data, usually 64 or 128 bits, to produce ciphertext.

④ Block cipher uses same key for encryption and decryption.

⑤ DES is best example of block cipher.

* Difference betn block & stream cipher.

| Block cipher | stream cipher |
|---|---|
| ① It is kind of encryption that convert plaintext by taking each block individual ly. | It is the kind of encryption that converts plaintext by taking one bytes of the plaintext at a time |
| ② feistel cipher is the most popular block cipher implementation. | vernam cipher is the main implementation of stream cipher |

Teacher's Signature

| | | |
|---|---|---|
| (3) | It is difficult to reverse encrypted text | It uses XOR encryption, which is easily reversed to plaintext. |
| (4) | Uses both confusion & diffusion | Relies on confusion only |
| (5) | ECB and CBC modes are used | CFB and OFB modes are used. |
| (6) | Complexity is Simple | Complexity is complex |
| (7) | 64 bits or more used | used 8 bits |

Q.9) write RSA algorithm? perform encryption using RSA algo., for the following p=7 q=11 e=3 M=9.

→ (1) RSA algorithm is an asymmetric cryptography algorithm.

(2) Asymmetric actually means that it works on two different keys ie. public and private key.

(3) public key is given to everyone and the private key kept private.

Teacher's Signature

Date .....
Page .....

④ The public key is used for encryption and the private key is used for decryption.

⑤ RSA is most common public-key algorithm, named after its inventors Rivest, Shamir and Adelman (RSA).

⑥

$p = 7 \quad q = 11 \quad e = 3 \quad M = 9$

$n = p * q$

$\therefore n = 7 * 11 = 77$

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

$\therefore \phi(n) = (7-1) * (11-1) = 6 * 10 = 60$

$d = e^{-1} \pmod{\phi(n)}$

$= 3^{-1} \pmod{60}$

$\therefore d = 27 \mod 60$

$\therefore d = 27$

To encrypt a message,

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

$= 9^3 \mod 77$

$= 729 \mod 77$

$\therefore C = 44$

Teacher's Signature _____

Q.10) write note on : ECC

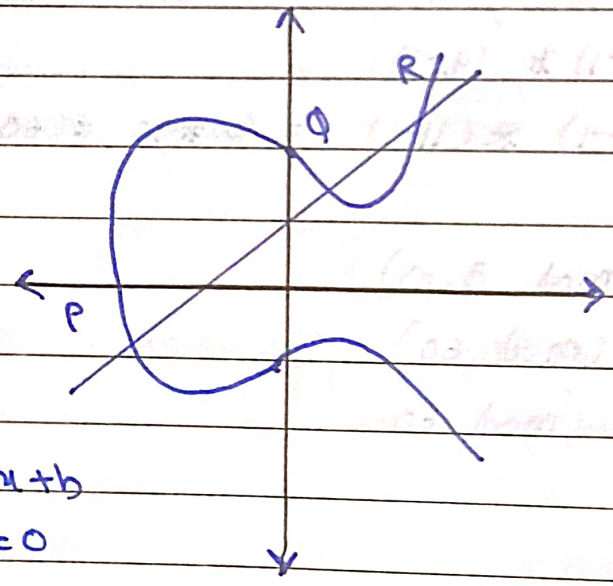
→ (1) ECC means Elliptic curve cryptography.

(2) It is a public-key encryption technique that uses pairs of public and private keys to encrypts and decrypt data.

(3) ECC is based on the mathematical theory of elliptic curves.

(4) It uses smaller keys than other cryptography methods to provide the same level of security.

(5) The encryption process take less time in ECC and decryption process takes more time.




$y = x^3 + ax + b$

$P + Q + R = 0$

Fig : Elliptic curve cryptography

(6) websites make extensive use of ECC to secure customers hypertext transfer protocol connection.

(7) ECC encryption is smaller, safer and faster.

Teacher's Signature

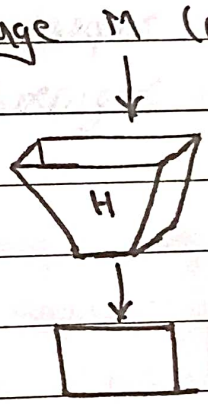
Q.11) Explain Hash function:

→ ① Hash function are extremely useful and appear in almost all information security application.

② A hash function is a mathematical function that converts a numerical i/p value into another compressed numerical value.

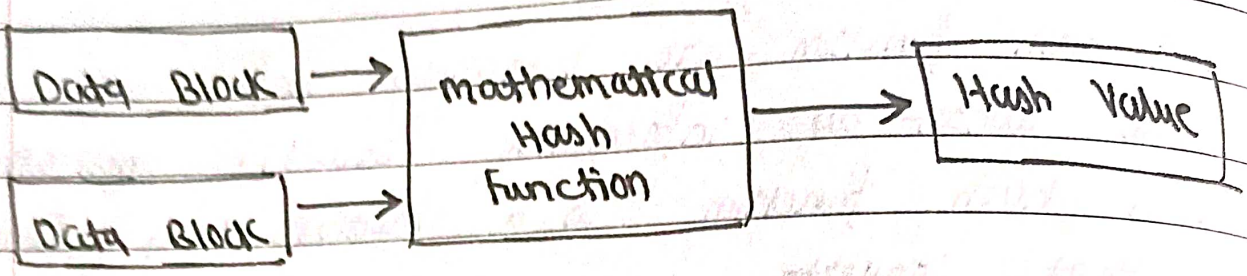
③ The i/p to the hash function is of arbitrary length but o/p has fixed length always.

④ Values returned by a hash function are called message digest or simply hash values.




⑤ Converting hash codes to their original value is an impossible task to perform. This is the main difference betn encryption as hash function.

Teacher's Signature _____

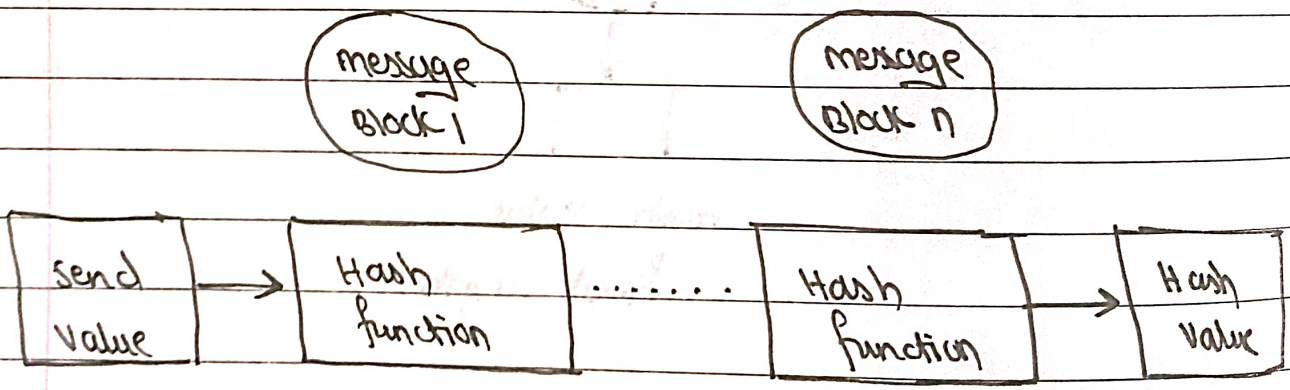



⑥ The size of each block varies depending on the algo.

⑦ Typically the block sizes are from 128 bits to 512 bits.

⑧ Hashing algo, involves rounds of above hash function like a block cipher.

⑨ The process is repeated for as many round as are required to hash the entire message..



Q.12) Describe Diffie - Hellman key exchange algorithm.

→ (1) The diffie - hellman key exchange algorithm is also known as exponential key exchange.

(2) It is method for securely exchanging cryptographic keys over an insecure channel.

(3) It is a fundamental building block of many secure communication protocols, including SSL / TLS and SSH.

(4) It is method for securely exchanging and used to established a shared communications while exchanging data over a public Networks using the elliptic curve to generate points and get the secret key using the parameter.

(5) The key exchange involves the following steps :-

i) Alice and Bob agree on two large prime no. p and g, and a public key exchange algo.

ii) Alice choose a secret integer a and computes $A = g^a \bmod p$. She sends A to Bob.

iii) Bob chooses a secret integer b and computes $B = g^b \bmod p$. He sends B to Alice.

iv) Alice computes $S = B^a \bmod p$. Bob computes $S = A^b \bmod p$.

v) Alice and bob now both have shared secret keys, which they can use to established a secured communication channel.

Teacher's Signature _____

Q. 13) Solve modular exponentiation algorithm:

(1) 23 power 3 mod 30.

→ $23^3$ mod 30

$= -7^3$ mod 30 || 23 mod 30 can be 23 or -7

$= -7^3$ mod 30

$= -7^2 \times -7$ mod 30

$= 49 \times -7$ mod 30

$= -133$ mod 30

$= -133$ mod 30

$= 17$

(2) 11 power 23 mod 187

→ $11^{23}$ mod 187

$= 11^{23} = 11 * 11 * 11 * 11^{20}$

$11 * 11 * 11 = 1331$ in to find this modulo 187 we look at 1331 / 187 which is > 7. so we can take $1331 - 7 * 187$ which is 22. So 11^3 mod 187 is 22. we can simplify $11^{23} = (11^3) * 7 * 11^2$ because we know $11^3 = 22$.

we can write this as $22 * 7 * 11^2$ and $11^2$ mod 187 is 121. so now have a no. to modulo.

$11 * 7 * 121$ mod 187 = 9317 mod 187

= 88

Teacher's Signature

Q.14) Explain the following terms :—→

i) Trap door and cross site scripting :

→ A back door or trap door, is a hidden entry to a computer device or s/w that bypasses security measures such as logins and password protections. It works in background and hides from the user. It is very similar to a virus and therefore is quite difficult to detect and completely disable.

Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web application. XSS enables attackers to inject client-side script into web pages viewed by other users. Attackers inject malicious script into a website. Attackers often initiate an XSS attack by sending a malicious link to user.

Teacher's Signature _____

(2) Host based v/s Network based IDS.

→

| | HIDS | NIDS |
|---|---|---|
| (1) | Host Intrusion Detection system | (1) Network Intrusion Detection System. |
| (2) | It doesn't work in real-time | (2) It operates in real time. |
| (3) | Response time is slow | (3) Response time is fast. |
| (4) | As it needs to be installed on every host, the installation process can be tiresome | (4) Few installation points make it easier to install NIDS. |
| (5) | HIDS can be installed on each and every computer server | (5) NIDS being concerned with network is installed at places like router or servers as these are the main intersection points in the network system. |

Teacher's Signature

Q.15 Short Notes on :

① PGP :→

① PGP stands for pretty good privacy, which is invented by phil zimmermann.

② PGP was design to provide all four aspect of security ie. privacy, integrity, authentication & non-repudiation in sending of emails.

③ PGP uses a digital signatures to provide integrity, non-repudiation and authentication.

④ PGP uses a combination of secret key encryption & public key encryption to provide privacy.

⑤ Therefore, we can say digital signature uses one hash function, on secret key and two private public key pairs.

⑥ PGP is an open source and freely available s/w package for email security.

⑦ Services offered by PGP are:

a) Authentication
b) Confidentiality
c) Compression
d) Email compatibility
e) Segmentation.

Teacher's Signature _____

(2) SQL injection: →

(1) SQL injection is a type of security vulnerability that occurs when an attackers is able to manipulate an SQL query in a way that allows them to gain unauthorized access to a database.

(2) This can lead to unauthorised data-access, data-manipulation and potentially even data deletion.

(3) SQL-injection is a common and dangerous attack vector, and web developers and database administrators needs to be aware of it and take step to prevent it.

(4) A successful SQL injection attack can result in unauthorised access to sensitive data, such as: password, credit sure details, personal user info..

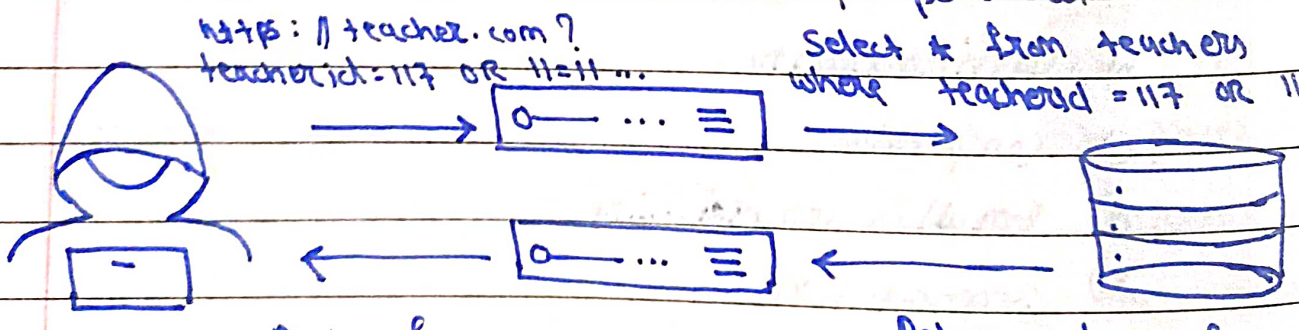



Fig: SQL Injection

Teacher's Signature _____

③ Chip Card Transaction :—→

→ ① Chip cards use cryptography to generate unique transaction codes that allow the terminal to authenticate the card.

② The card uses its private key to generate a digital signature of the transaction details and send this back to the reader.

③ The cards's chip contains a digital certificate that is used to verify the authenticity of card.

④ During a transaction, the card generates a cryptogram that is based on the transaction data and a secret key stored on the card.

⑤ A chip card is a debit or credit card that contains an embedded microchip along with the traditional magnetic stripe.

Teacher's Signature _____

Q.16) Chinese problem:

Apply the chinese Remainder Theorem to solve following congruent Equation.

$x \equiv 2 \pmod 3$

$x \equiv 3 \pmod 5$

$x \equiv 2 \pmod 7$

↳

$m_1 = 3 \quad m_2 = 5 \quad m_3 = 7$

$a_1 = 2 \quad a_2 = 3 \quad a_3 = 2$

1) Common modulus M:

$M = m_1 * m_2 * m_3$

$= 3 * 5 * 7$

$= 105$

2) $M_1 = \frac{m}{m_1} = \frac{105}{3} = 35$

$M_2 = \frac{m}{m_2} = \frac{105}{5} = 21$

$M_3 = \frac{m}{m_3} = \frac{105}{7} = 15$

Teacher's Signature

3) $M_1^{-1} = 35^{-1} \pmod 3 = 2$

$M_2^{-1} = 35^{-1} \pmod 5 = 1$

$M_3^{-1} = 35^{-1} \pmod 7 = 1$

4)

$$x = ((a_1 * m_1 * m_1^{-1}) + (a_2 * m_2 * m_2^{-1}) + (a_3 * m_3 * m_3^{-1})) \bmod 105$$

$= ((2 * 35 * 2) + (3 * 21 * 1) + (2 * 15 * 1)) \bmod 105$

$= (140 + 63 + 30) \bmod 105$

$= 233 \bmod 105$

$= 23$

$\therefore 23 \bmod 3 = 2$

$\therefore 23 \bmod 5 = 3$

$\therefore 23 \bmod 7 = 2$

} cross checking ...

Teacher's Signature _____