NAME: SAMRUDDHI NEVREKAR.
ROLL NO.: 3029

M T W T F S S
Page No.:
Date:
YOUVA

M2 - ISP.

Q1.)

1)

→ 1) Diffie - Hellman key exchange, also called exponential key exchange, is a method of digital encryption that uses number raised to specific powers to produce decryption keys on the basis of components that are never directly transmitted, making the task of a would-be code breakers mathematically overwhelming.

2) As the name suggests, This algorithm is used to exchange the secret key between the sender and the receiver.

3) This algorithm facilitates the exchange of secret key without actually transmitting it

4) Eg: Credit card transaction email

2)

→ Given

$n = 17$

$a = 5$

Private key of Alice = 4

Private key of Bob = 6

Step 1 :-

Public key of Alice $= 5^{\text{Private key of Alice}} \bmod 17$

$= 5^4 \bmod 17$

$= 13$

Public key of Bob $= 5^{\text{Private of Bob}} \bmod 17$

$= 5^6 \bmod 17$

$= 2$

Step 2 :-

Secret key obtained by Alice $= 2^{\text{Private key of Alice}} \bmod 7$

$= 2^4 \bmod 17$

$= 16$

secret key obtained by Bob = $13^{\text{Private Key of Bob}} \bmod 7$

$= 13^{16} \bmod 17$

$= 16$

The value of common secret key = 16.

3)

→ Encryption

The plaintext (P) and key(K) are added modulo 26

$E_i = (P_i + K_i) \bmod 26$

Decryption

$D_i = (E_i - K_j + 26) \bmod 26$

4)

→
```
x = lambda a,b : a*b
print (x(5,6))
```

Q2)

→ To implement Diffie-Hellman, the two end users Alice and Bob, while communicating over a channel they know to be private, mutually agree on positive whole numbers p and q such that p is the prime number and q is generator of p. The generator is a number that, when raised produces the same result for any two such whole number. The value of p may be large but the value of q is usually small.

Alice	Bob
1) Public key available = P, G	1) Public key available = P, G
2) Private key selected = a	2) Private key selected = b

3) Key generated = $x = G^a \bmod P$
4) Exchange of generated keys
5) Key received = y
6) Generated secret key =
$K_a = y^a \bmod P$

3) Key generated $y = G^b \bmod P$
4) Same as Alice.
5) Key received = x
6) Generated secret key =
$K_b = x^b \bmod P$

Algebraically, it can be shown that
$K_a = K_b$.

Q3)

→ 1) Vigenere cipher is method of encrypting alphabetic text. It uses a simple form of polyalphabetic substitution.
2) A polyalbetic cipher is any cipher based on substitution, using multiple substitution alphabets.
3) The encryption of the original text is done using the vigenere square or vigenere table
4) The table consists of the alphabets written out 26 times in different row, each alphabets shifted cyclically to the left compared to the previous alphabet, corresponding to the 26 possible Ceasar cipher.

Input : Plaintext : GEEGSFORGEEKS
Keyword : Samruddhi
Output : Ciphertext : GCYZFMLYLEIM
For generating key, the given keyword is repeated in a circular manner.
The keyword "Samruddhi" generates the key "SAMRUDHISAMRU"

Q4)

```
string = "GEEKSFORGEEKS"
keyword = "samruddhi"
def generatekey (string, key):
    key = list (key)
    if len (string) == len (key):
        return (key)
    else:
        for i in range (len (string) - len (key)):
            key.append (key[i % len (key)])
    return ("".join (key))
def encrypt_cipherText (string, key):
    cipher_text = []
    for i in range (len (string)):
        x = (ord (string[i]) + ord (key[i])) % 26) + ord ('A')
        cipher_text.append (chr (x))
    return ("".join (cipher_text))

key = generatekey (string, keyword)

print ("Original Message", string)
print ("Keyword:" keyword)
cipher_text = encrypt_cipherText (string, key)
print ("Cipher text:", cipher_text)
```

Original Message: GEEKSFORGEEKS
Keyword: Samruddhi
ciphertext: YESTXZYDWZ