Name → Aditya Vellore
Roll no - 5046.
SapID - 70522100088
Subject - ISP

~~Q1) Diffie Hellman key exchange is used as an algorithm~~

Q1) ① Diffie - Hellman key exchange is a method of digital encryption which produces decryption keys using specific powers to certain numbers.
② It is also called exponential key exchange
③ The basic idea behind this is that the encryption code should not be hacked while transmission.
④ Examples ⇒ ~~Gi~~ Credit card transcation mails,

Q2) $q = 17$
$\alpha = 5$ = root

Public key of alice

$= 5^4 \bmod 17$
$= 16\ 2$

Secrit key obtained by bob
$= 2^4 \bmod 17$
$= 16$

Values of Secret Key of both bob and alice is 16

~~Sec~~ Secret Key = 16

Option - A.

Secret key obtained by Alice
$= 13^6 \bmod 17$
$= 16$

Camlin Page
Date / /

Q3) Encryption formula for Vigenere Cipher ⇒

The plain text(A) and key(K) are added mod 26

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

Decryption ⇒

$$D_i = (E_i - K_i + 26) \bmod 26.$$

Q4) X = Lambda a, b : a * b
print(x(5,6))

Output : 30

Q2) Steps for Diffie-Hellman ⇒
To implement key exchange ⇒

Vaibhav and Nigati are two end users, while communication over a channel they know to be private, and hence mutually agree on positive whole numbers A, and B. Such that A is a prime number and B is a generator of A. The generator B is a number that, when raised to positive whole-numbers powers less than A, never produces the same result for any two such whole numbers the value of A maybe large but the value of B is usually small.

Alice

Public keys available = P, G

Private key selected = a

key generated =

$x = g^a \bmod P$

Exchange of generated keys takes place

key received = y

Generated Secret key

$k_a = y^a \bmod P$

Bob

Public key available = P, G

Private key selected = b

key generated

$y = g^b \bmod P$

key received = x

Generated Secret key

$k_b = x^b \bmod P$

Vigenere cipher is a method of encrypting alphabetic text. It uses a simple form of polyalphabetic substitution.

Apolyalphabetic cipher is any cipher based on substibution, using multiple substitution alphabets. The encryption of the original text is done by using the Vigenere square or Vigenere table.

The table consists of the alphabets written out 26 times in different rows, each alphabet shifted cyclically to the left compared to the previous alphabet, corresponding to the 26 possible Caesar ciphers. At different points in the encryption process, the cipher uses a

alphabet from one of the rows. The alphabet used at each point depends on repeating keyword.

Input : Plaintext: Geeks for Geeks
keyword : Mandar
Output Ciphertext: GCYCZFMLYLEIM
For generation key, the given keyword is repeated in a circular manner until it matches the length of the plain text.

keyword "Mandar" generates the key "MandarMGLE".

Q4) Encryption code for Vigenère cipher.

```
String = "Geeks for Geeks"
keyword = "SHARAN"

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 encryptCipherText(string, key):
    Cipher_text = []
    for i in range(len(string)):
        x = (ord(string[i]) + ord(key[i])) % 26)
                + ord('A')
        Ciphertext.append(chr(x))
```

```
return ("".join(cipher_text))

key = generateKey(string, keyword)

print("Original Message", string)
print("Keyword:", keyword)
cipher_text = encryptCipherText(string, key)
print("CipherText:", cipher_text)
```

Original Message GeeksforGeeks
Keyword : Sharon
CipherText : SLEBSSGYYGVEXK