SUBJECT:_____ PAGE NO.:_____

NAME: Mandar Rele ROLL NO.:_____ STD:_____ DIV:_____

TOPIC:_____ DATE:_____ TERM:_____ ASSIGNMENT NO.:_____

I.S.P M.2 5036

1 Question - 1

(1) → Diffie Hellman key exchange, also called exponential key exchange, is a method of digital encryption that uses numbers raised to specific powers to produce decryption keys on the basis of components that are never directly transmitted, making the task of a a would-be code breaker mathematically overwhelming.
eg:- credit card transaction email

(1) (2) $n = 17$

$a = 5$

private key of Alice = 4

private key of Bob = 6

public key of Alice

$= 5^4 \bmod 17$

$= 13$

public key of bob

$= 5^6 \bmod 17$

$= 2$

Secret key obtained by Alice

$= 2^4 \bmod 17$

$= 16$

Secret key obtained by Bob

$= 13^6 \bmod 17$

$= 16$

The value of common secret key = 16

(A)

SUBJECT:_____ PAGE NO.:_____

NAME:_____ ROLL NO.:_____ STD:_____ DIV:_____

TOPIC:_____ DATE:_____ TERM:_____ ASSIGNMENT NO.:_____

1 (3) encryption

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

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

decryption

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

1 (4)

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

2] QUESTION-2

→ 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 number p and q, such that p is a prime number and q is a generator of p, the generator q is a number that when raised to positive whole number powers less than p, never produces the same result for any 2 such whole numbers. The value of p may be large but the value of q is usually small.

Alice	Bob
Public keys are : P, G	Public keys = P, G
Private selected key = a	Private key selected = b
key genarated = $x = G^a \bmod P$	key genarated = $y = G^b \bmod P$
exchange of genaratid keys takes place	
key received = y	key received = x
genarated secret keys	
$k_a = y^a \bmod P$	$k_b = x^b \bmod P$

algebraically it can be shown

$k_a = k_b$

SUBJECT:_____ PAGE NO.:_____

NAME: Mandar Rele ROLL NO.:_____ STD:_____ DIV:_____

TOPIC:_____ DATE:_____ TERM:_____ ASSIGNMENT NO.:_____

I.S.P M.2 5036

Q3.) Question - 3

→ Vignere cipher is a method of encrypting alphabetic text. It uses a simple form a polyalphabetic substitution. A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets. The encryption of the original text is done using the vigenere square a 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 different alphabet from one of the rows. The alphabet used at each point depends on a repeating keyword.

Input : plain text :- GEEKSFOR GEEKS
Keyword :- AYUSH

Output :- Ciphes text :- GCYCZFMLYLEIM

The keyword ~~ayush~~ AYUSH genarates the key AYUSHAYUSHAYU

for genarating key, the given keyword is repeated in a circular manner until it matches the length of the plain text

SUBJECT:_____ PAGE NO.:_____

NAME:_____ ROLL NO.:_____ STD:_____ DIV:_____

TOPIC:_____ DATE:_____ TERM:_____ ASSIGNMENT NO.:_____

Q4] QUESTION-4

```
string = "GEEKSFORGEEKS"
keyword = "SHARAN"

def generatidKey (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 = generatidKey(string, keyword)
print ("Original Message", string #)
print ("Keyword:", keyword)
cipher_text = encrypt_cipherText(string, key)
print ("Ciphertext:", cipher_text)
```

Original Message :- GEEKSFORGEEKS
Keyword :- SHARAN
Cipher Text : YLEBSSGYGVEXK