Roll no: 5039
Name: Rishi Shah

ISP

Q1] Diffie - Hellman is also known as exponential key exchange and it is a method of digital encryption that uses numbers raised to specific powers to produce a decryption keys. on the basis of the components that are never directly transmitted. This is used to exchange the secret key between the sender and reciever. The algorithm ~~facilities the~~ facilitates the exchange of secret key without actually transmitting it.

Q2] $n = 17$

$p = 5$

$kA = 4$

$kB = 6.$

Public key of Alice $= 5^4 \% 17$

$= 13.$

Public key of Bob $= 5^6 \% 17$

$= 2$

Secret key of Alice $= 2^4 \bmod 17$

$= 16.$

Secret key of Bob $= 13^6 \bmod 17$

$= 16.$

Common secret key = 16.

Option 1.

3] Encryption:

~~The~~ plaintext = P

key = K

Encrypt = E

$$E = (P + K) \bmod 26$$

Decryption = D

$$D = (E - K + 26) \bmod 26.$$

4]
```
a = lambda x,y : x*y
    print (x(2,1))
```

2] For Diffie-Hellman both users should know ~~to~~ be private and mutually agree on positive whole number p & q. such that p is a prime number and q is a generator of p. q is a number that when raised to positive whole-number powersless than p, never produces the same result for any two such whole nos. The value of p may be large but the value of q is usually small.

X	Y
PublicKey = P, G	Public key = P, G
Private key = a	Private key = b.
key generated	key generated
$x = G \bmod P$	$y = G \bmod P$
Exchanged of keys take place	
Key recieved = y	key recieved = x.
Secret key Generated	secret key Generated
$k_a = y^a \bmod P$	$k_b = x^b \bmod P.$

$k_a = k_b.$

Q3] It is a method of encrypting alphabetic text. It uses a simple form of 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 Vigenère square or Vigenere table.
The table consists of 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 Cipher.
At different points in the encryption process, the cipher uses a different alphabet from one of the rao. The alphabet used at each point depends on a repeating keyword.

Input: Plaintext : GEEKS FORGEEKS
keyword : AYUSH
Output: Ciphertext: GCYCZFMLYLEIM

For generating key, the given key word is repeated in a circular manner unit it matches the length of plaintext
The keyword "AYUSH" generates key "AYUSHAYUSH AYU"

Encryption:
The plaintext (P) and key (K) are added modulo 26
$E_i = (P_i + K_i) \bmod 26.$

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

Q4]
```
string = "GEEKSFORGEEKS"
keyword = "SHARAN"

def generate_key(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_cipher Text(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= generate Key (string, keyword)

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

```
Original message : GEEKSFORGEEKS
Keyword: SHARAN
Ciphertext: YLEBSSGYGVEXK
```