Babu Madhav Institute of Information Technology
Unit Test - 1
Sem - 5 Div - B

Page No. 1
Date : 1-10-20

Date of Exam :- 1-10-20 Time of Exam :-
Subject Code :- 0600010509 Subject Name :- Information Security
Enrollment :- 201806100110127 Name :- Vishwa Chaturvedi

Q to A.

(I) The Key difference between Stream cipher and block cipher is that the stream cipher is stretched into long stream bits whereas block cipher is into the block of words.

Stream cipher = bits (letter-by-letter)
Block cipher = words (block of words)

(II) Kerckhoff's principle :- The inner working of the cryptosystem are completely known to attacker, only the secret is the Key.

(III) Code book cipher refers to the kind of book usually additive words and random numbers that means a book filled with code words.

Eg: If we set a particular code for specific words =

Vishwa - Image
Sleeping - car

(P.T.O.)

Page No. 2
Date : 1-10-25

Q1

I

Then after using code book the sentence will be:-

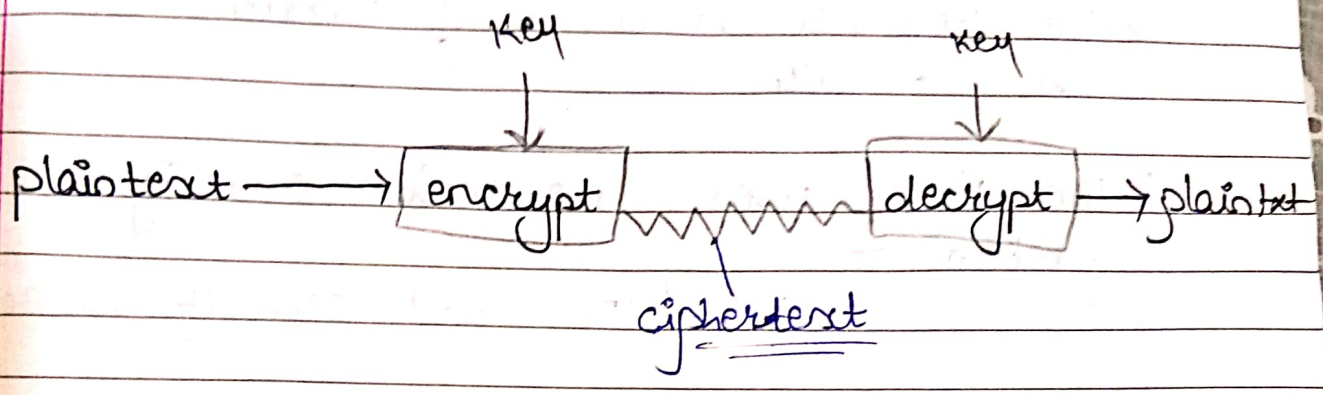
plaintext = Vishwa is sleeping
ciphertext = Tnuge is fab

IV Advantage of CBC Mode:-

(1) In CBC Blocks and plain text are encrypted Based on ciphertext of previous Blocks

Q1 B

I Crypto as Black Box refers to key crypto in which encryption & decryption is done




II Substitution cipher:-

1. VKJ, ACUUWVML, BIW XZMMBQ

⇒ dsr iKccedutJefhuuJy

2. QFE LQY HVIWLJDWLRQ

⇒ tth dthKyzOMgzOUT

| A | B | C | D | E | F | G | H |
|---|---|---|---|---|---|---|---|
| d | e | f | g | h | i | J | K |
| I | J | K | L | M | N | O | P |
| L | M | N | O | P | Q | R | S |
| Q | R | S | T | U | V | W | X |
| T | U | V | W | X | Y | Z | A |
| Y | Z | | | | | | |
| B | C | | | | | | |

Page No. 4
Date : 1-10-20

## III RC4

⇒ RC4 is a stream cipher, optimized for software implementation.

⇒ The key size must be of variable size in RC4

⇒ The RC4 uses Network security protocol –
SSL / TLS web security protocol

⇒ NOw, RC4 produces a key stream that is XORed with the plain text.

- There are two algorithms in RC4

1. Initialization of RC4
2. RC4 encryption.

⇒ The initialization phase

```
for i = 0 to 255
  S[i] = i
  K[i] = key [ i mod N]
  Next i
  j = 0
for i = 0 to 255
```

$j = (j + S[i] + K[i]) \bmod 256$

Swap

Next i

$i = j = 0$

After the initialization phase the "Keystream" byte is generated.

This "Keystream byte" can be XORed with plaintext for encryption and XORed with ciphertext for decryption

Q2. A.

⇒ plaintext = "Harry will attack in June"

5*5

| | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| 1 | H | a | r | r | y |
| 2 | w | i | l | l | a |
| 3 | t | t | a | c | k |
| 4 | i | n | J | u | n |
| 5 | e | x | x | x | x |

Row

i n J un
t t a c k
w i l l a
H a r r y
e

Column

n i J n v
t t a k c
9 w l a l
a H R y R
x c x x x

ciphertext = nijnuttackimalahrajr-e

Q2. B.

plaintxt=
I T D E P T R A I D S A T R A J I V A K O R A O F F I C E

* Value of N ?
* where N is used in "key" to encrypt

Page No. 7
Date :

Q3

B. 3 DES / triple DES

the 3DES means use 2 keys in E - DE sequence

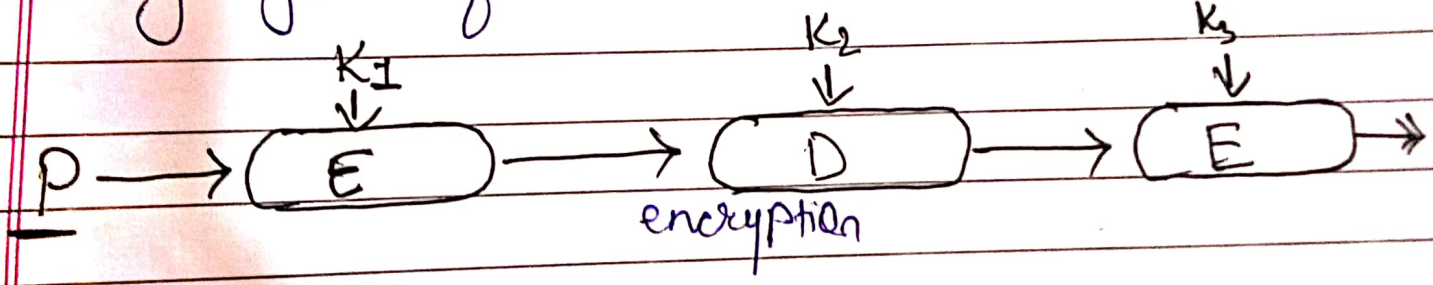
$K_1$ = Key 1
$K_2$ = Key 2

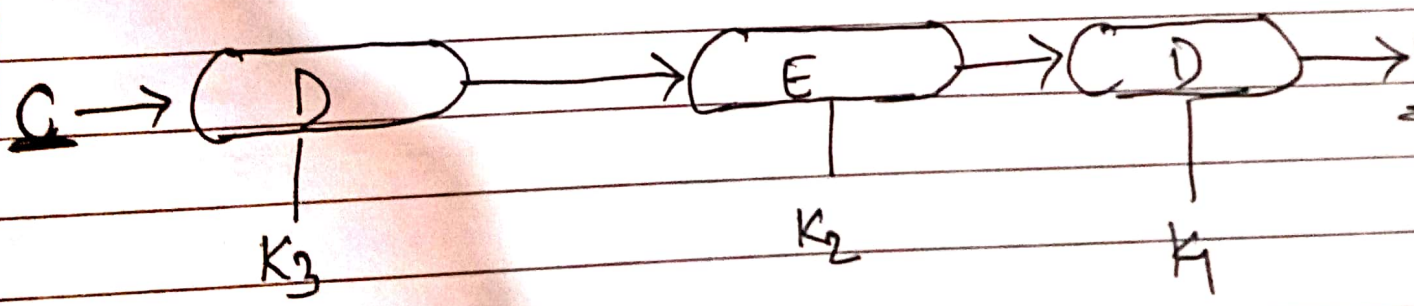
therefore $C = E_{K1} - D_{K2} - E_{K3} - P$

use 3 keys and 3 execution of DES algorithm (encrypt - decrypt - encrypt)

★ Effective key length =

Keylength of 168 bit



Page No. 8
Date :

Q3 c.

DES- Data encryption standard

→ DES is the most widely used encryption scheme.

→ The algorithm of DES is reffered to the "Data encryption algorithm".

- DES is Block cipher. The DES is fiscal cipher with 64 bit block length, 56 bit key length, 16 rounds of encryption / decryption and 48 bits of key used in each round.

The security of DES depends heavely on S-Box