ID: 18DCS007 UNIT TEST II

NAME: RUDRA BARAD SUB: CNS

DATE: 19/4/21

Q1. Example of Invertible S-Box.

If the input to the left box is 001 then output is 101

The input 101 in the right table creat the output 001. which shows that the two tables are inverse of each other.

↓ 3 BITS

	00	01	10	11
0	011	101	111	100
1	000	010	001	110

↓ 3 bits

Table for encryption

↓ 3 BIT

	00	01	10	11
0	100	110	101	000
1	011	001	111	010

↓ 3 bits

Table used for decryption

Q2. ID : 18DCS007 → 18007

CIPHER KEY → 18007
+ 45
18052

(18052)$_{10}$ → (1000110100001100)$_2$

taking 1st 10 bits as key

NAME : RUDRA BARAD

Plain Text = RUDRABAR
Key = 1000110100

→ Applying initial permutation

Initial Permutation

4	5	2	7	9	10	1	3	8	6

I/P = 1000110100
O/P = 0100001011

→ Apply circular left shift on both halves

I/P = 01000 01011
O/P = 00100 10101

→ Apply compression D-Box

6	3	1	4	10	5	7	9

I/P = 0010010101
O/P = 11001000
↳ K_1

(3) 18DCS007

→ Apply shift left operation on o/p on step (2)

I/P = 00100 10101
O/P = 01000 01010

~~Here we have to apply two shift~~

→ Apply compression D-Box

| 6 | 3 | 1 | 4 | 10 | 5 | 7 | 9 |

I/P = 0100001010
O/P = 00000011
↳ K_2

PLAINTEST : RUDRABAD

↓ ↓ ↓

17 2 3

17 − 10001
20 − 10100

↙ ↓

10001 10100

→ APPLY INITIAL PERMUTATION

I/P = 10001 10100
O/P = 01010011

∴ L = 0101 R = 0011

→ APPLY SDES FUNCTION ON RIGHT BOX

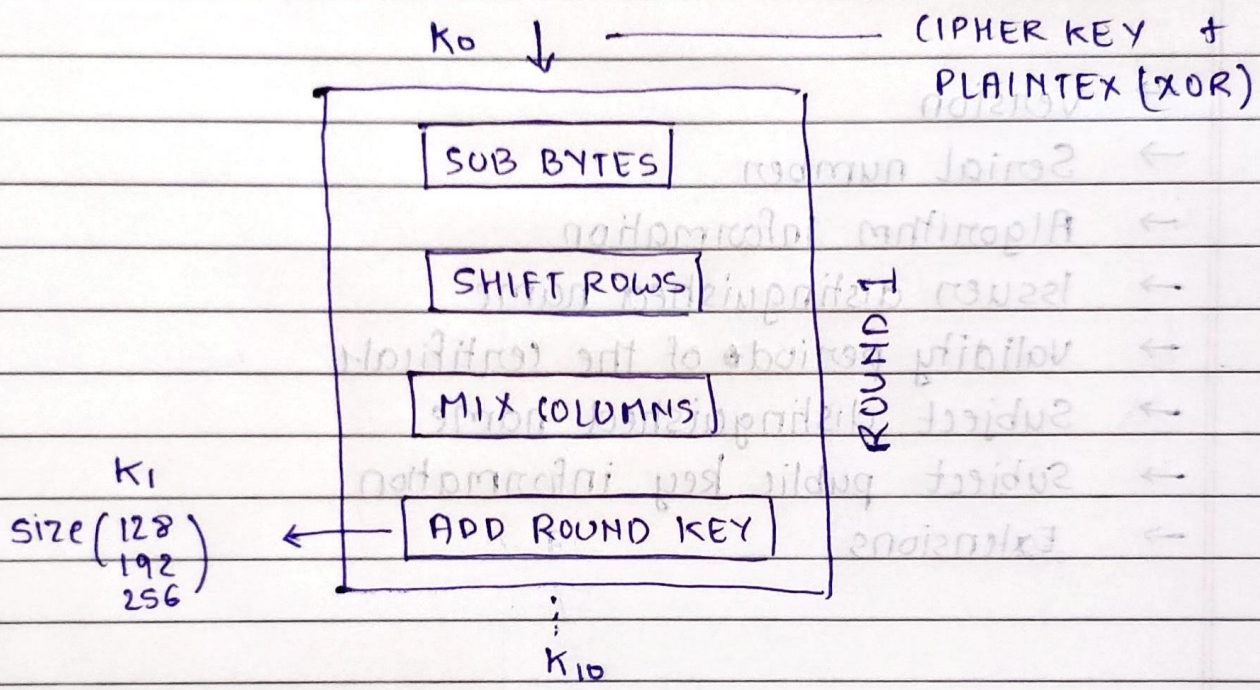
I/P = 0011
O/P = 00110011

18DCS007

Q3. In AES there are variable rounds according to the size of key used.

KEY SIZE	NO. OF ROUNDS
128	10
192	12
256	14.

DIAGRAM OF A ROUND IN AES



STEPS IN EACH ROUND

1. SUBSTITUTION OF BYTES - byts of block text are substituted based on rules dictated by pre-defined S-boxes

2. SHIFTING ROWS - next comes permutation stp. In this stp, all rows exiept the first are shifted by one.

3. MIXING OF COLUMNS - In 3rd step, Hill cipher is used to jumble up the message more by mixing block's columns.

4. ADDING ROUND KEY - In final step, the message is XORed with the respective round key.

Miracle
Page
Date

Q4. CIPHER BLOCK CHAINING - It is an advancement on ECB since ECB compromises some security requirements.

In this previous cipher block is given as input to next encryption algorithm after XOR with original plaintext block.

CIPHER FEEDBACK MODE - In this mode cipher is given as feedback to the next block of encryption with some new specifications.

First an initial vector IV used for first encryption & output bits are divided as set of s and b bits the left hand side s bits are selected are applied an XOR operation with plaintext bits.

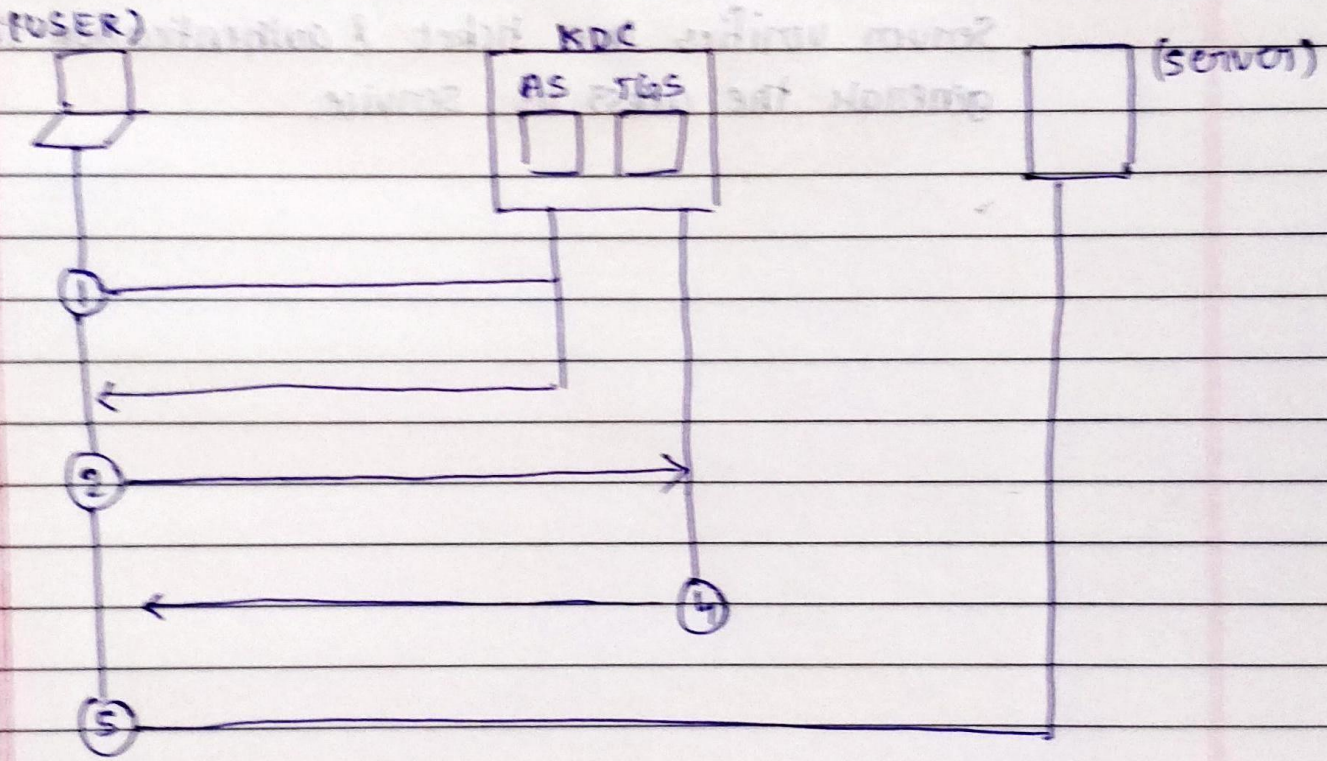
18DCS007

Q5 KERBEROS is an authentication protocol and a KDC. It has become very popular.

Servers included in Kerberos are following:

(1) An authentication server AS
(2) Ticket Granting Server (TGS)
(3) Real Data server that provides services to others (Bob)

KERBEROS GENERAL MODEL



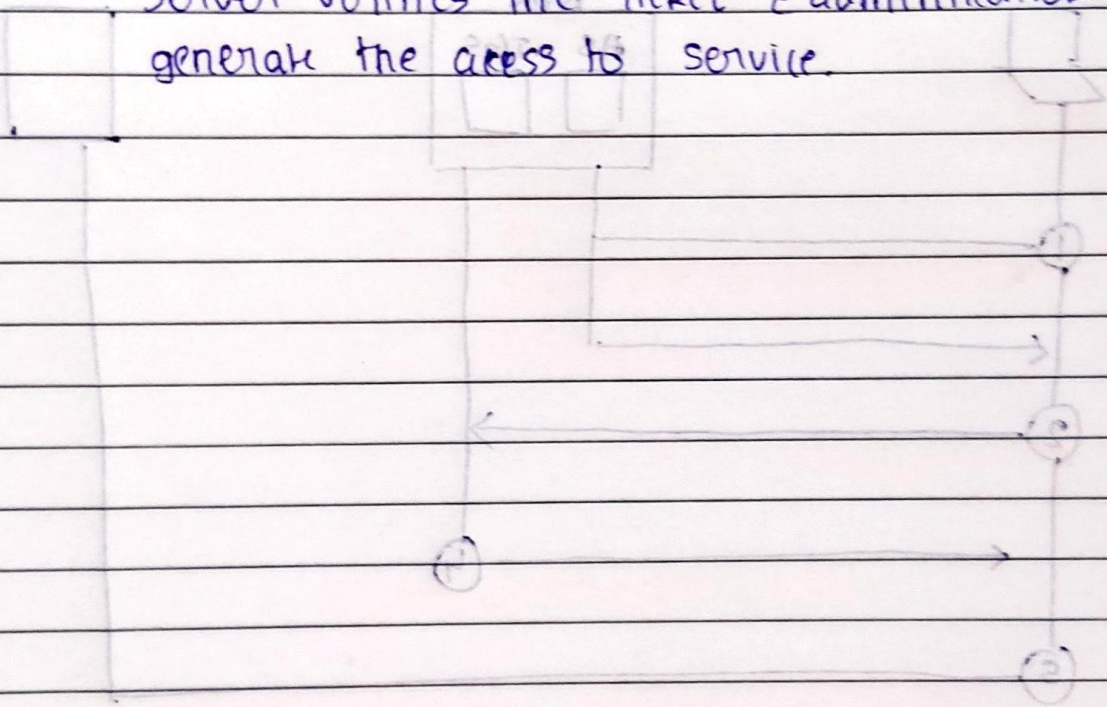
STEP 1: user logon and request service on host. Thus user request for ticket-granting service

STEP 2: Authentication service verifies user's access right using database and then gives ticket-granting ~~service~~ and session key. Results are encrypted using password

STEP 3: Decryption of message is done using password then send ticket to ticket granting server. Ticket contain authentications like username & network address.

STEP 4: Ticket Granting server decrypts ticket send by user & authentication verifies request then creates ticket for requesting services from server

STEP 5: User send the ticket & authentication to server. Server verifies the ticket & authentication then generate the access to service.



18DCS007

Miracle
Page
Date

Q6. INTRODUCER TRUST:

→ In real life we do not trust on people that we don't know. PGP solves this problem by providing levels of trust.

→ The introduction trust specifies what level of trust the introducer wants to allocates to others users in the system.

CERTIFICATE TRUST:

→ When a user A receives certificate of another user B issued key by third person C depending on the level of trust that A has in C. A assigns certificate trust level while storing it.

KEY LEGITIMACY:

→ The objective of introducers trust & certif. trust is to decode whether to trust the public key of the user. In PGP it is called as key legitimacy.

18DCS007

Q7.

MD5	SHA-512
→ MD5 stands for digest	→ Stands for secure hash algorithm
→ Can have 128 bits length of message digest	→ Can have 512 bits length of message digest
→ Speed is fast, as compared to SHA-512	→ Speed is slow as compared to MD5
→ Provides poor security	→ Has complex architecture
→ Was presented in 1990's, is old	→ It is comparatively modern new
→ 2^{128} operations needed	→ 2^{512} operations

Q8. An x.509 certificate is a digital certificate that uses widely accept international x.509 public key infrastructure standard to verify that a public key belongs to user.

An x.509 certificate contains information about identity to which a certificate is issued & identity that issued it. Standard information in an x.509 certificate includes:

→ Version
→ Serial number
→ Algorithm Information
→ Issuer distinguished name
→ Validity period of the certificate
→ Subject distinguished name
→ Subject public key information
→ Extensions