Name : Sradha Kedia

Date of Examination : 18 December, 2021

Time of Examination : 9:30 am to 1:30 pm

Examination Roll no. : 20234757053

Semester : III

Unique Paper Code : 223401302

Title of Paper : Information Security

Email-Id : 200083@cs.du.ac.in

Mobile no. of student : ~~200083@cs.du.ac.in~~ 9899519848

Question no. : 2

No. of pages : 4

Name of the program : MCA

Name of the Department : DUCS

Ans 2. (i) S-boxes are generally used to provide non-linearity in a modern block ciphers but IDEA cipher does not use S-box. IDEA is an iterated block cipher that operates on using 8 rounds and 128 bit key on 64 bit blocks. The algorithm employs 3 mathematical operations: XOR, addition modulo 2^{16}, and Lai-Massey multiplication. this mixed mode arithmatic is used to achieve the required non-linearity & mixing (i.e. both Confusion and diffusion)

plaintext 1001 1100 1010 1100
key 1101 1100 0110 1111 0011 1111

We have a 16 bit plain text & 24 bit key which is divided into 4 & 6 blocks of 4 bit each

$x_1 = 1001$ $K_1 = 1101$
$x_2 = 1100$ $K_2 = 1100$
$x_3 = 1010$ $K_3 = 0110$
$x_4 = 1100$ $K_4 = 1111$
$K_5 = 0011$
$K_6 = 1111$

① $X_1 * K_1$ $(1001\,(9) * (1101)(13))(\text{mod } 17) = 1111\,(15)$
② $X_2 + K_2$ $(1100\,(12) + (1100)(12))(\text{mod } 16) = 1000\,(8)$
③ $X_3 + K_3$ $(1010\,(10) + (0110)(6))(\text{mod } 16) = 0000\,(0)$
④ $X_4 * K_4$ $(1100\,(12) * (1111)(15))(\text{mod } 17) = 1010\,(10)$
⑤ ① ^ ③ $(1111\,(15) \wedge (0000)(0)) = 1111\,(15)$
⑥ ② ^ ④ $(1000\,(8) \wedge (1010)(10)) = 0010\,(2)$
⑦ ⑤ * K_5 $(1111\,(15) * (0011)(3))(\text{mod } 17) = 1011\,(11)$
⑧ ⑥ + ⑦ $(0010\,(2) + (1011)(11))(\text{mod } 16) = 1101\,(13)$

(9) (8) * K_6 (1101 (13) * 1111(15)) (mod 17) = 1000(18)

(10) (7) + (9) (1011 (11) + 1000(8)) (mod 16) = 0011(3)

(11) (1) ^ (9) (1000(8) ^ {1111 (15)) = 0111(17)

(12) (3) ^ (9) (1000 (8) ^ 0000 (0)) = 1000(8)

(13) (2) ^ (10) (0011 (3) ^ 1000 (8)) = 1011 (11)

(14) (4) ^ (10) (0011 (3) ^ 1010 (10)) = 1001 (9)

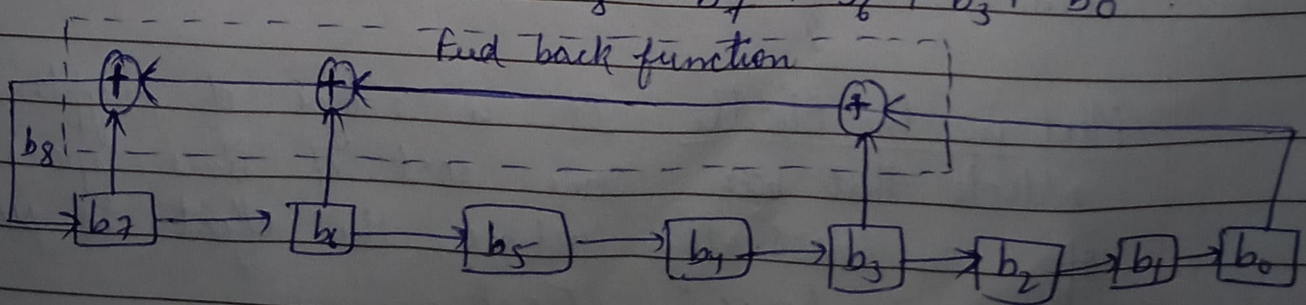
The input to next round is step 11 || step 13 || step 12 || step 14

0111 || 1011 || 1000 || 1001 (12 & 13 are interchange because After each complete round 12 and 13 swap except for the last round. After interchanging we get (11) | (13) | (12) | 14

$\boxed{\text{Round 1 output} \quad 0111 \ 1011 \ 1000 \ 1001}$

2 (ii) LFSR is a shift operator that has some of its output together in XOR configurations to form a feedback path. LSFRs are frequently used as pseudo random pattern generators to generate a random numbers of 1's and 0's

LSFR with 8 cells $b_8 = b_7 + b_6 + b_3 + b_0$.



A LFSR is a shift register whose input bit is a linear function of its previous state. the only linear func. of single bits is XOR, thus its is a shift register whose input bit is driven by the exclusive or of some bits of the over all shift register value.

likewise, because the register has a finite no. of possible states. It must eventually enter a repeating cycle. However, an LFSR with well chosen feedback function can produce a sequence of bits which appears random and which has a very long cycle.

They are ① used as counters.
② used in cryptography.
③ used in digital broadcasting & communications.

(iii) Man in the middle - It is an active attack to a cryptographic protocol where the attacker is efficiently in b/w the communication of two users and is capable of intercepting, relying and altering messages. In the case the meaning of in the middle is direct, the attacker is in the middle of two communicating users.

Meet in the Middle: It is a type of cryptanalytic attack that uses some sort of time-space trade off to drastically reduce the effort to perform a brute-force attack.

① The biggest difference between these attacks is that first one is interactive (i.e. attacker must participate in communication) while the second is not.

② While names are similar, a MITM attack is very different from meet in the middle because MITM involves a malicious user eavesdropping or altering the conversion between 2 or more individual in carry out an attack. The attacker in this cases takes a position in the middle of an exchange while hiding or disgusting their activity so they can intercept and possible alter data flowing back & forth.