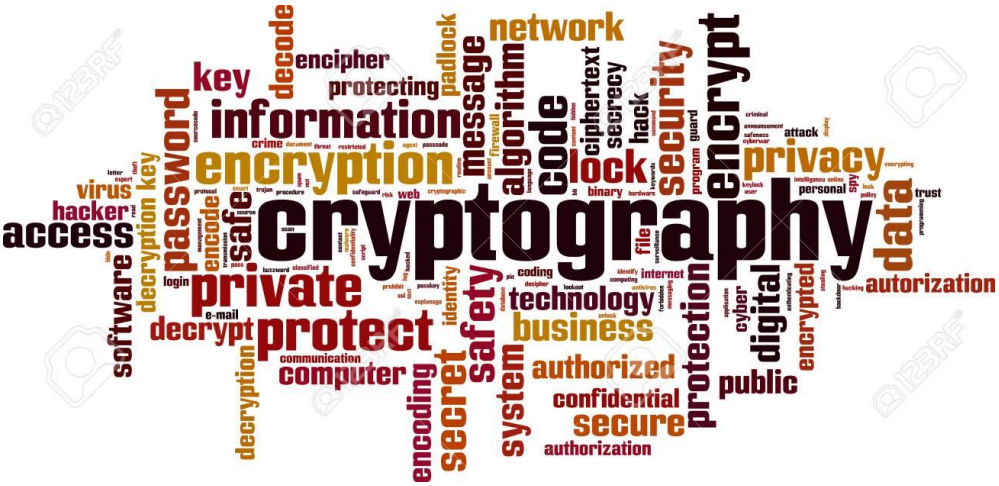
CRYPTOGRAPHY

CSPC-35



04/04/2021

Assignment - 2

Submitted By: -

106118085 - Sampurn Anand

106118105 - Manvitha Vunnam

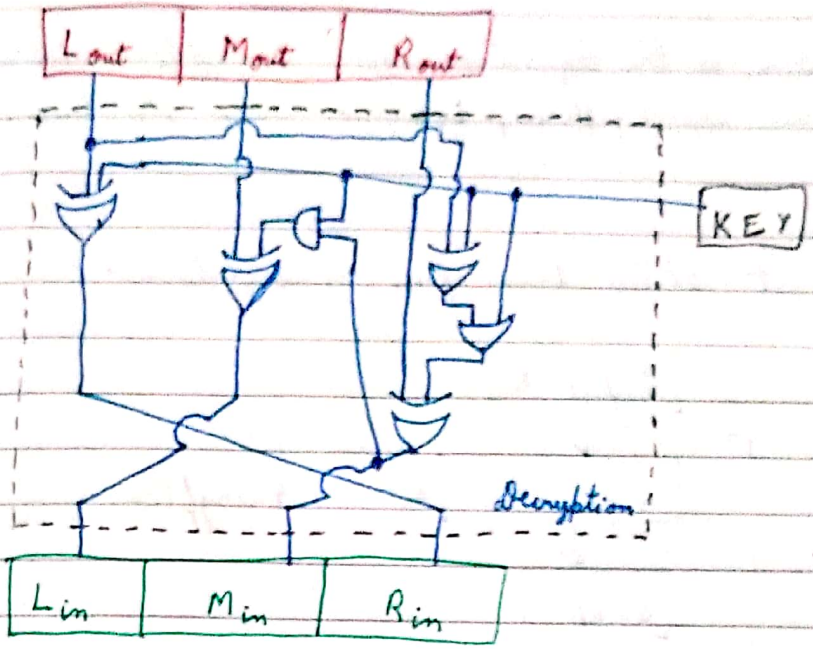
106118115 - Sabrina Rahman

106118073 - Pavitra Visvanatharoa

106118027 - Raja Yadidiah

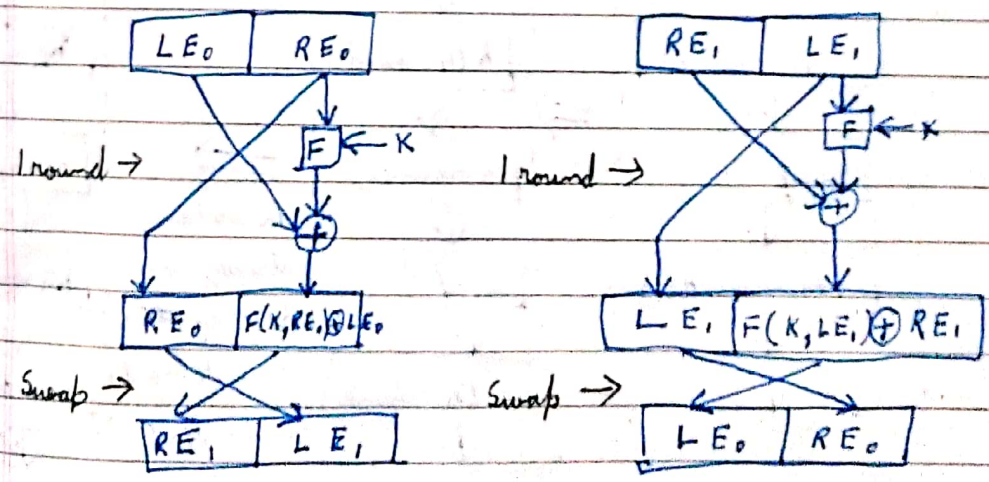
106118085
CSE-A
Sarfaraz Anand

1)



2) a) To prove :- Encryption is similar to decryption in DES.
That is, for one round it will be,
$LE_0 = RE_1 \oplus F(K_1, LE_1)$, and will continue so on for any number of rounds

Proof :- For one round :-



Encryption Decryption

Clearly, for encryption :-

$RE_1 = LE_0 \oplus F(K, RE_0)$ — (i)

and $LE_1 = RE_0$ — (ii)

(i) and (ii) $\Rightarrow$ $RE_1 = LE_0 \oplus F(K, LE_1)$

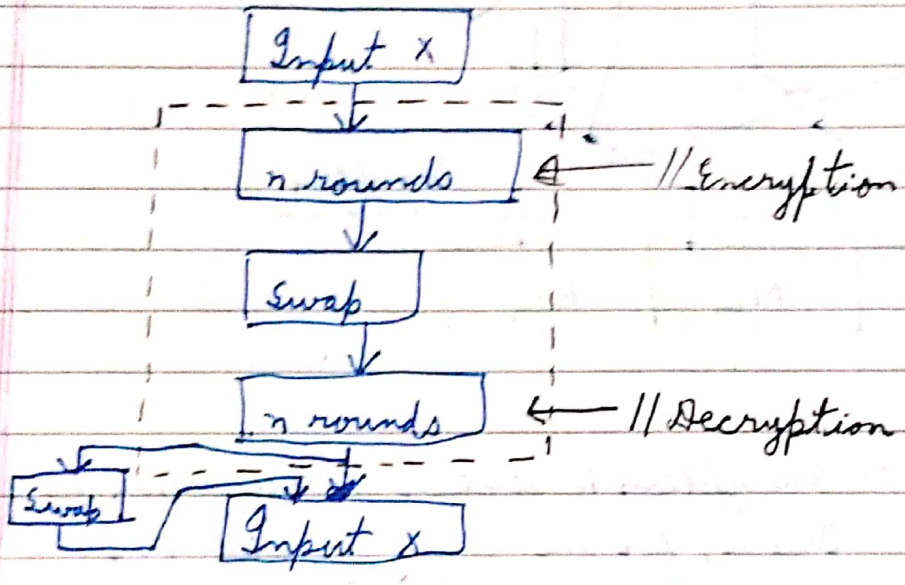
$\Rightarrow$ $RE_1 \oplus F(K, LE_1) = LE_0 \oplus F(K, LE_1) \oplus F(K, LE_1)$

$\Rightarrow$ $LE_0 = RE_1 \oplus F(K, LE_1)$

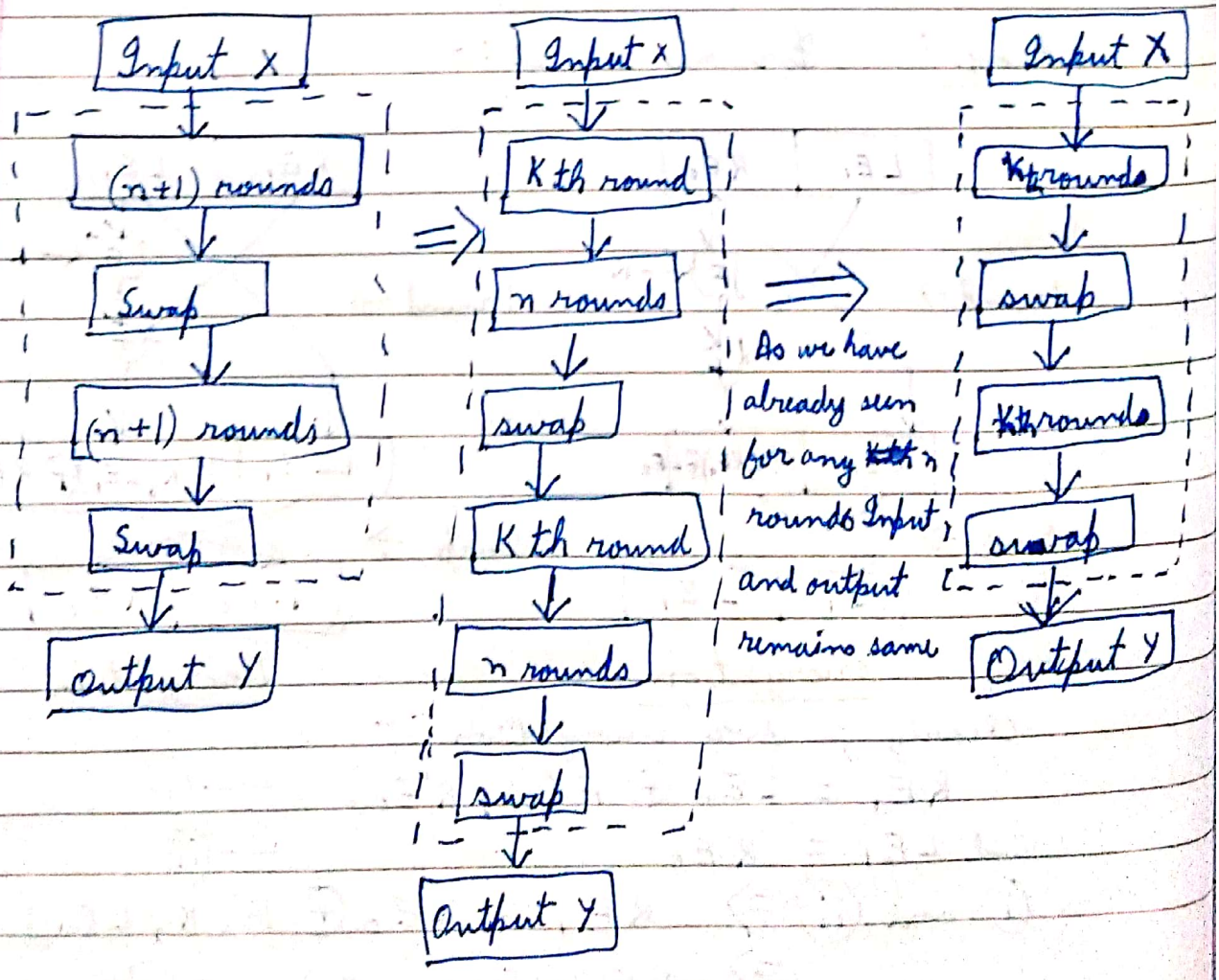
This is the equation for decryption in case of one round. Hence, for one round its true.

Now,

Let it be true for n rounds :-



For n+1 rounds :-



This is same as for 1 round, so, DES decryption is similar to Encryption for any cases.

b) Given → $Y = E(K, X)$

where, Y = Encrypted text

K = Key

X = Plain text

X' = Complement of X (Bitwise)

To prove → $Y' = E(K', X')$

Proof → Let $X = L_i || R_i$, and $Y = L_{i+1} || R_{i+1}$

DES Encryption gives :-

$L_i = R_{i-1}$ —— (i)

$R_i = L_{i-1} \oplus F(R_{i-1}, K)$ —— (ii)

(i) $\Rightarrow$ $L_i' = R_{i-1}'$ —— (iii)

(ii) $\Rightarrow$ $R_i' = [L_{i-1} \oplus F(R_{i-1}, K)]'$

$= [L_{i-1}' \oplus F(R_{i-1}, K)]$

$[\because (A \oplus B)' = A' \oplus B]$

Also,

$F(R_{i-1}, K)' = F(R_{i-1}', K')$

$\therefore R_i' = [L_{i-1}' \oplus F(R_{i-1}', K')]$ —— (iv)

(iii) & (iv) $\Rightarrow$ $Y' = E(K', X')$ —— (A)

Hence, proved.

c) In the case of ~~brte~~ brute-force attack on DES,

Key Size = 56 (Key space searching)

$\Rightarrow$ Total no. of keys = 256

$\Rightarrow$ Complexity of the attack = $O(256)$

In case of chosen plaintext attack,

$M_1 \longrightarrow C_1 = DES_{K_1}(M_1)$

$M_1' \longrightarrow C_2 = DES_{K_1}(M_1')$

From (A) :-

$C_2' = DES_{K_1'}(M_1)$

$\therefore \quad M_1 \rightarrow C_1 (K_1)$

$M_1 \rightarrow C_2' (K_1')$

Now trying the permutations of key :-

If M_1 gives C_1 with $K \longrightarrow$ The key is K

If M_1 gives C_2' with $K \longrightarrow$ The key is K'

else K and K' are not keys

$\Rightarrow$ In ~~worst~~ worst case, both keys are wrong.

$\therefore$ Search key space of K is reduced by half, so the complexity is $O(256/2) = O(128)$

3) In 3-DES,

Size of key = 56

When brute-force is applied, the time complexity $= O(2^{168})$

Using "Meet in Middle" attack, it can be reduced

$$M \longrightarrow E_{K_1}[M] \longrightarrow E_{K_2}[E[M]] \longrightarrow E_{K_3}[E[E[M]]] = C$$

The middle place happens after the plaintext is encrypted twice and where ciphered text is decrypted twice.

Time complexity of each event of cryptanalysis :-

a) ~~Time to~~ For encrypting the plaintext twice $= O(2^{112})$

[2 sets of Keys $\rightarrow K_1, K_2$]

b) Decrypting the ciphertext once $= O(2^{56})$ (Key K_3)
c) Sorting the set of ciphertexts $= O(2^{56} * \log(2^{56}))$
d) Comparing K_1, K_2 and K_3 $= O(2^{112} * \log(2^{56}))$

Total time complexity

$= O(2^{112}) + O(2^{56}) + O(2^{56} * \log(2^{56})) + O(2^{112} * \log(2^{56}))$

$= O(2^{112} * \log(2^{56}))$

$= O(2^{112} * 56) \simeq O(2^{112} * 2^6)$

$= O(2^{118})$

4) A block cipher works by replacing N bits from the plaintext with a block of N bits from the ciphertext.
If N = 4, then 16 different 4-bit patterns are possible.
Each pattern can be represented by an integer between 0 and 16, i.e.,

0000 → 0
⋮
1111 → 15

In ideal block cipher, the input blocks are randomly related to output blocks. It is invertible to decrypt and are one-to-one. The encryption key for the ideal block cipher is the table containing relationship b/w input and output blocks.

If keys (K_1 & K_2) map 2 different input blocks to two different output blocks, then they will give same results only if $K_1 = K_2$.
If $K_1 \neq K_2$, then
P(Keys (K_1, K_2) giving same pair of plaintext & ciphertext)
$= 0$

5) $Z_7 = (1, 2, 3, 4, 5, 6) * \text{mod } 7$
$= (3^0, 3^2, 3^1, 3^4, 3^5, 3^3)$

∵ Z_7 can be written as powers of its element = 3.

⇒ Z_7 is a cyclic group.

Identity element = 1

$2^{-1} = 4$, $3^{-1} = 5$

$\langle 1 \rangle = 1$
$\langle 2 \rangle = 2, 4, 1$
$\langle 3 \rangle = 3, 2, 6, 4, 5, 1$
$\langle 4 \rangle = \langle 2 \rangle = 2, 4, 1$
$\langle 5 \rangle = \langle 3 \rangle = 3, 2, 6, 4, 5, 1$
$\langle 6 \rangle = 6, 1$

∴ Required cyclic ~~sof~~ subgroups are : 1, 2, 4, 1, 3, 2, 6, 4, 5, 1, 6 and 1.

6) $H = (0, 1, 2, 3, 4, 5, 6, 7) + \text{mod } 8$

$\langle 0 \rangle = 0$
$\langle 1 \rangle = 1$
$\langle 2 \rangle = 2, 4, 0$
$\langle 3 \rangle = 3, 1$
$\langle 4 \rangle = 4, 0$
$\langle 5 \rangle = 5, 1$
$\langle 6 \rangle = 6, 4, 0$
$\langle 7 \rangle = 7, 1$

∴ Required cyclic subgroups are : 0, 1, 2, 4, 0, 3, 1, 4, 0, 5, 1, 6, 4, 0, 7 and 1.

Since, no subgroup contains all elements = H is not a cyclic group.

7) A Schnorr group, proposed by claus P Schnorr is a large prime-order subgroup of Z_p^*, the multiplicative group of integers modulo p for some prime p. To generate such a group, generate p, q, r such that

$$p = qr + 1 \quad \text{with } p, q \text{ prime.}$$

Then choose any h in the range $1 < h < p$ until you find one such that

$$h^r \neq 1 \pmod{p}$$

This value

$$g = h^r \bmod p$$

is a generator of a subgroup of Z_p^* of order q. We are given that $p = 11 = 2 * 5 + 2$ ($2^2 = 4$, $4 \bmod 11 = 4 \neq 1$).

$g = h^r \bmod p = 2^2 \bmod 11 = 4 \bmod 11 = 4$.

Generator (g) = 4

The elements of the schnorr group are: $\{4^1, 4^2, 4^3, 4^4, 4^5, 4^6, 4^7, 4^8, 4^9, 4^{10}\}$ 4, 5, 9, 3, 1, 4, 5

8) Properties of a Ring:

1. First operation

(a) This should be a group with respect to this operation

2. Second operation:

(a) Must be closed under this operation.

(b) Must be associative under this operation.

(c) Must be commutative under this operation.

3. The two operations must satisfy Distributive law.

Properties of a field:

1. First operation:

(a) This should be a group with respect to this operation.

(b) Should be commutative.

2. Second operation.

(a) Must be closed under this operation.

(b) Must be associative under this operation.

(c) Must be commutative under this operation.

(d) Identity must exist for all elements of the set.

(e) Inverse must exist for all polynomials of the set, except for the identity element of the first operation.

3. The two operations must satisfy distributive law.

Proofs:

1. First operation:

(a) This should be a group with respect to this operation. This already holds good, as this group is a ring.

(b) Should be commutative. This is given as a commutative Ring. Therefore, this condition is taken care of.

2. Second operation:

(a) Must be closed under this operation. This is in properties of Ring and is thus satisfied

(b) Must be associative under this operation. This is in properties of Ring and is thus satisfied.

(c) Must be commutative under this operation. This is in properties of Ring and is thus satisfied.

(d) Identity must exist for all elements of the sets. This is in properties of Ring and is thus satisfied.

(e) Inverse must exist for all polynomials of the set, except for the identity element of the first operation. Identity element of first addition operation: 0. Identity element of second multiplication element: 1. Inverse element of polynomial $\sum_{i=0}^{4} a_i x^i$, $a \in Z_{18}$ for second multiplication

operation is obtained by applying Euclidean algorithm to the polynomial and x^q+1 and equating it to their GCD which is 1(This will be true as x^q+1 is a prime polynomial). Inverse will have to exist because R is a ring with unity, which means that any element u that has an inverse element in the multiplicative monoid of R, i.e, an element v such that $uv = vu = 1_R$, where 1_R is the multiplicative monoid R, i.e., an element however will not be possible to apply on 0 and x^q+1 as it will result in division by zero, Thus, we can say that inverse does not exist for zero element, which is the identity for first addition operation. Thus, this condition holds true.

3. The two operations must satisfy Distributive law. this is in properties of Ring and is thus satisfied.

We have proved that R is a field.

9) Properties of a Ring:

1. First operation:

(a) This should be a group with respect to this operation

2. Second operation:

(a) Must be closed under this operation.

(b) Must be associative under this operation.

(c) Must be commutative under this operation.

3. The two operations must satisfy Distributive law.

properties of a Field:

1. First operation:

(a) This should be a group with respect to this operation.

(b) Shoud be commutative.

2. Second operation:

(a) Must be closed under this operation.

(b) Must be associative under this operation.

(c) Must be commutative under this operation.

(d) Identity must exist for all elements of the set.
(e) Inverse must exist for all polynomials of the set, except for the identity element of the first operation.
3. The two operations must satisfy Distributive law.
proofs:

1. First operation:
(a) This should be a group with respect to this operation. This already holds good, as this group is a ring.
(b) Should be commutative. this is given as a commutative Ring. Therefore, this operation is taken care of.
2. Second operation:
(a) Must be closed under this operation. This is in properties of Ring and is thus satisfied.
(b) Must be associative under this operation. This is in properties of Ring and is thus satisfied.
(c) Must be commutative under this operation. This is in properties of Ring and is thus satisfied.
(d) Identity must exist for all elements of the set. This is in properties of Ring and is thus satisfied.
(e) Inverse must exist for all polynomials of the set, except for the identity element of the first operation.
Identity element of first addition operation: 0. Identity Element of second multiplication Element: 1. Inverse element of polynomial $\sum_{i=0}^{q} a_i x^i$, $a \in Z_{11}$ for second multiplication operation is obtained by applying, Euclidean algorithm to the polynomial and x^4+1 and equating it to their GCD which is 1 (This will be true as x^4+1 is a prime polynomial). Inverse will have to exist because R is a ring with unity, which means that any element will have to exist because R is a that has an inverse element in the multiplicative monoid of R, i.e. an element v such that $uv = vu = 1_R$, where 1_R is the multiplicative identity. This method however will not be possible to apply on 0 and x^4+1 as it will result in division by zero. Thus we can say that inverse does not exist for 0 Elem-ent.

which is the identity for first addition operation. Thus, this condition holds true.

3. The two operations must satisfy Distributive law. This is in Properties of Ring and is thus satisfied.

We have proved that R is a field.

10) This field with 9 elements starts with the integers mod3, forms polynomials with coefficients in the integers mod3, and then looks at only the remainders of these polynomials when divided by an irreducible (prime) polynomial of degree two in GF(3). Since we assume that there exists some irreducible polynomial in every degree, let there be a 2 degree polynomial which is irreducible in GF(3). Let this irreducible polynomial be.

$$x^2+1$$

Substituting 0, 1 and 2 in the above polynomial, we see that they are not roots and hence the polynomial is irreducible in GF(3) the elements of GF(9) are therefore:

$$\{0, 1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2\}$$

This properties of the field can be checked as follows with the operations being + mod 3 and * mod 3. Examples of addition.

$$1+2=0$$

$$(x)+(2x+1)=1$$

$$(2x+2)+(2x+2)=2(2x+2)=x+1$$

Examples of multiplication.

$$2*2=1$$

$$x*2=2x$$

$$x*x=x^2=x^2+2(x^2+1)=3x^2+2=2$$

11) Additive and multiplicative inverse of x^3+x+1 in GF(24), with prime polynomial $= x^4+x+1$

Additive inverse is itself

$= x^3+x+1$

$[(x^3+x+1)+(x^3+x+1)] \bmod 2^4 = 0$

we can find multiplicative inverse by extended Euclidean Algorithm

let $r_0 = x^4+x+1$

$r_1 = x^3+x+1$

$r_2 = r_0 - q_1 r_1 \qquad q_1 = \left[\frac{r_0}{r_1}\right]$

$x+1 = r_0 - x r_1$

$r_3 = r_1 - q_2 r_2$

$1 = r_1 - x r_2$

$r_4 = r_2 - q_3 r_3$

$0 = r_2 - (x^2+1) r_3$

$\therefore GCD(r_0, r_1) = 1$

Inverse exists

$r_1 - x r_2 = 1$

$r - x(r_0 - x r_1)$

$= r_0(x) + r_1(x^2+1)$

$\therefore r_1^{-1} \bmod r_0 = x^2+1$

$(x^3+x+1)^{-1} \bmod (x^4+x+1) = x^2+1$

$x^3+x+1 \overline{)x^4+x+1}$ (quotient x)

x^4+x^2+x

x^2+1

$x^2+1 \overline{)x^3+x+1}$ (quotient x)

x^3+x

1

$1 \overline{)x^2+1}$ (quotient x^2+1)

x^2+1

0

Verification :-

$(x^3+x+1)(x^2+1) \bmod (x^4+x+1)$

$(x^5+x^3+x^3+x+x^2+1) \bmod (x^4+x+1)$

$$x^4+x+1 \;\overline{)\; x^5+x^2+x+1 \;\big|\; x}$$
$$x^5+x^2+x$$
$$1$$

Multiplicative inverse $= x^2+1$

(2) prime polynomial $= x^3+x+1$

(i) x^2+2x+1

Extended Euclidean algorithm

let $r_0 = x^3+x+1$

$r_1 = x^2+2x+1$

$r_2 = r_0 - q_1 r_1 \qquad q_1 = \left[\frac{r_0}{r_1}\right]$

$x = r_0 - (x+1) r_1$

$r_3 = r_1 - q_2 r_2$

$1 = r_1 - (x+2) r_2$

$r_4 = r_2 - q_3 r_3$

$0 = r_2 - x r_3$

$x^2+2x+1 \;\overline{)\; x^3+x+1 \;\big|\; x+1}$
x^3+2x^2+x
x^2+1
x^2+2x+1
x

$\text{GCD}(r_0, r_1) = 1$

Inverse Exists

$x \;\overline{)\; x^2+2x+1 \;\big|\; x+2}$
x^2
$2x+1$
$2x$
1

$1 = r_1 - (x+2) r_2$

$1 = r_1 - (x+2)(r_0 - (x+1) r_1)$

$1 = r_1 - (x+2) r_0 + (2x+1)(2x+2) r_1$

$1 = r_1 + (2x+1) r_0 + (x^2+2x+x+2) r_1$

$1 = (2x+1) r_0 + x^2 r_1$

$1 \;\overline{)\; x \;\big|\; x}$
x
0

$r_1^{-1} \bmod r_0 = x^2$

$(x^2+2x+1)^{-1} \bmod x^3+x+1 = x^2$

Verification

$(x^2+2x+1)(x^2) \bmod x^3+x+1$

$x^4+2x^3+x^2 \bmod x^3+x+1$

$$x^3+x+1 \;\overline{)\; x^4+2x^3+x^2 \;}\; x+2$$

$$x^4+x^2+x$$

$$2x^3+2x$$

$$2x^3+x+2$$

$$1$$

$\therefore$ Multiplicative inverse $= x^2$

(ii) $2x+2$

Let $r_0 = x^3+x+1$

$r_1 = 2x+2$

$r_2 = r_0 - q_1 r_1$

$2 = r_0 - (2x^2+x+1) r_1$

$r_3 = r_1 - q_2 r_2$

$0 = r_1 - (x+1) r_2$

$GCD(r_0, r_1) = 2$

Inverse does not exists.

$$2x+2 \;\overline{)\; x^3+x+1 \;}\; 2x^2+x+1$$

$$x^3+x^2$$

$$2x^2+x+1$$

$$2x^2+2x$$

$$x+1$$

$$x+2$$

$$2$$

$$2 \;\overline{)\; 2x+2 \;}\; x+1$$

$$2x$$

$$2$$

$$2$$

$$0$$

13)

Ans: no of machines $= \frac{4 * 10^{12}}{200}$

$= 2 * 10^{10}$

no of keys processed per sec $= 10^9 * (2 * 10^{10})$

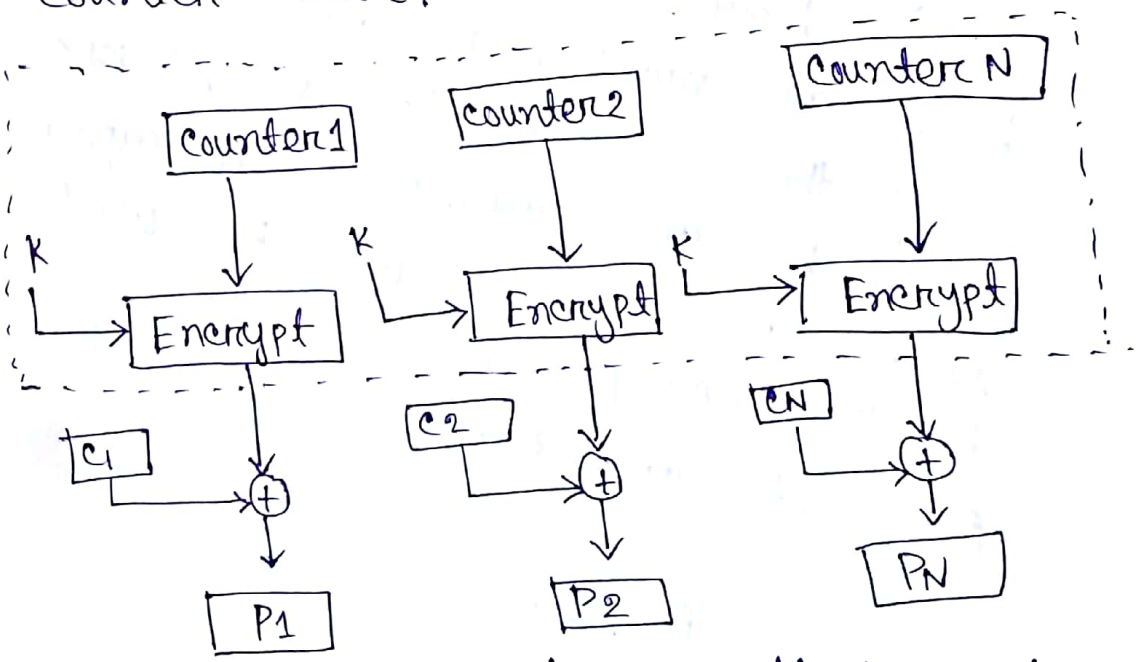
$= 2 * 10^{19}$

no of seconds $= \frac{2^{128}}{(2 * 10^{19})} = 1.7 * 10^{19}$

This many seconds is about 540 billion years.

14)

Ans: Decryption is a randomized counter mode:

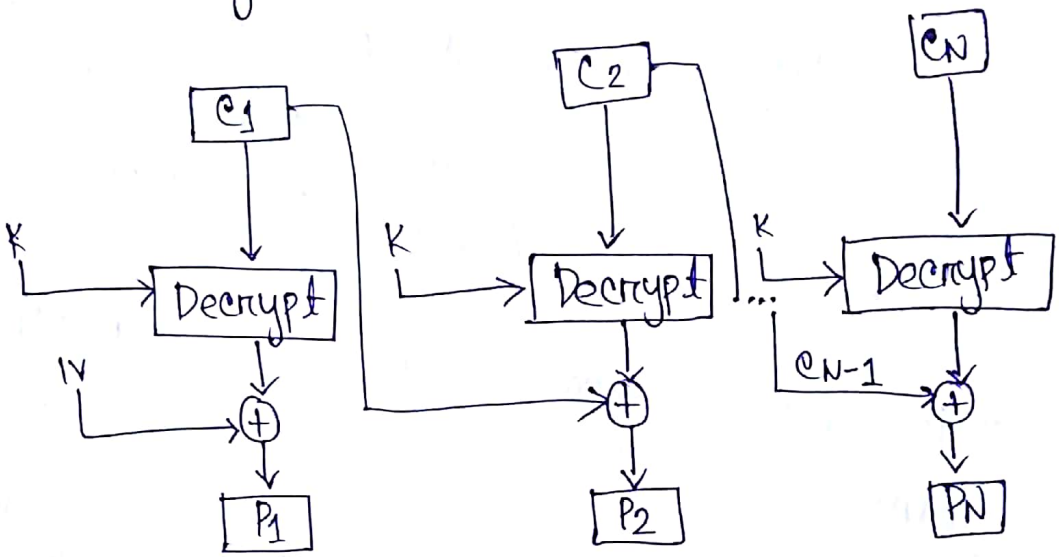


Each ciphertext block affects only the current block. So when a ciphertext block at number 1/2 gets corrupted only 1/2 will be corrupted.

Answer is 1.

15)

Ans: Decryption in a cipher Block Chaining mode:



~~Eea~~ Each ciphertext block affects only the current block and the next block. So, when a ciphertext block at number K gets corrupted only the plaintexts K and K+1 will be ~~cou~~ corrupted as ciphertext at block K will be used in the computation of the Plaintext at K+1.

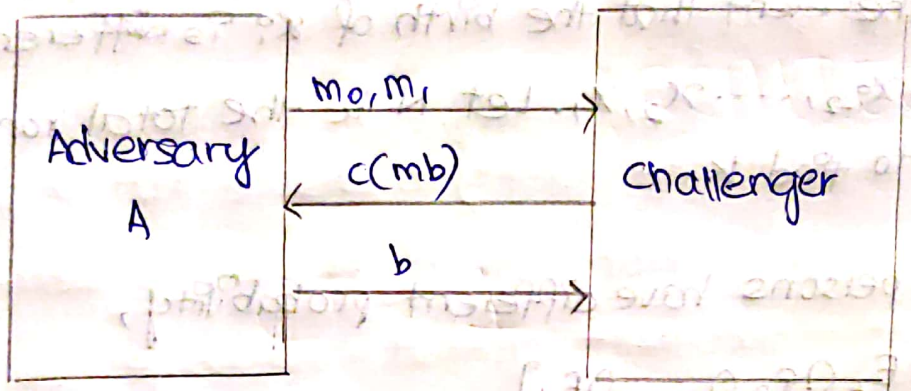
Answer is 2.

CRYPTO ASSIGNMENT-2

By: 106118073 PAVITRA VISVANATHAROA.

(16) Prove that block cipher with ECB mode is not semantically secure.

Ans:



* c represents encryption using ECB mechanism and b is either 0 or 1.

ECB mode is not IND-CPA and hence not semantically secure. The above figure shows the construction of an attacker A. A picks any two messages m_0 and m_1 of same lengths and sends them to the challenger. The challenger picks a random bit b and encrypts (in ECB mode) the message mb and sends the corresponding cipher text c back to A. A simply queries the encryption oracle one of the messages, say m_0, and obtains the corresponding cipher text c_0. If $c_0 = c$, then A sets $b_0 = 0$, else it sets $b_0 = 1$. A then sends b_0 to the challenger. It is easy to see that since ECB mode yields a deterministic scheme, the advantage of A is exactly 1. Hence ECB is not semantically secure.

(17) Find the minimum value of k (minimum no. of students) such that probability is greater than 0.5 that atleast two people in a group of k-people have the same birthday? How it improves the attack on collision resistant property of the hash function?

Sol: Let E_i denote the event that the birth of x_i is different from birthday of $x_{i-1}, x_{i-2}, \ldots x_2, x_1$. Let N be the total range in which we have to find k.

Probability that all persons have different probability,

$$P[N,k] = P[E_1 \cap E_2 \cap E_3 \cap \ldots \cap E_N]$$

Using Baye's theorem,

$$= P\left[\frac{E_2 \cap E_3 \cap \ldots \cap E_N}{E_1}\right] * P[E_1]$$

$$= P\left[\frac{E_3 \cap \ldots \cap E_N}{E_2 \cap E_1}\right] * P\left[\frac{E_2}{E_1}\right] * P[E_1]$$

$$= P\left[\frac{E_N}{E_1 \cap E_2 \cap \ldots \cap E_{N-1}}\right] \ldots * P\left[\frac{E_3}{E_2 \cap E_1}\right] \times P\left[\frac{E_2}{E_1}\right] \times P[E_1]$$

$$P[E_1] = \frac{N}{N}$$

$$P[E_2] = \frac{N-1}{N}$$

$$\vdots$$

$$P[N,k] = \frac{N-k+1}{N} \times \ldots \frac{N-2}{N} \times \frac{N-1}{N} \times \frac{N}{N}$$

$$= \frac{N}{N} \times \frac{N-1}{N} \times \frac{N-2}{N} \times \ldots \frac{N-k+1}{N}$$

$$= \frac{N}{N} \times \left[1 - \frac{1}{N}\right] \times \left[1 - \frac{2}{N}\right] \times \ldots \left[1 - \frac{k-1}{N}\right]$$

using $e^{-x} = 1 - x$ (for low values of x)

$$= \exp\left[\frac{-(1+2+\ldots+(k-1))}{N}\right]$$

Probability that two persons have same birthday,

$$= 1 - \exp\left[\frac{-(1+2+\ldots+(k-1))}{N}\right]$$

$$= 1 - \exp\left[\frac{-k(k-1)}{2N}\right]$$

To have probability greater than 0.5,

$$1 - \exp\left[\frac{-k(k-1)}{2N}\right] \approx \frac{1}{2}$$

$$k \approx 1.18\sqrt{N}$$

In a year $N = 365$, so $k = 1.18 \times \sqrt{365} = 22.54$ which is very close to the correct answer of 23. In essence, if we choose random variables from a uniform distribution in the range 0 through $N-1$, then the probability that a repeated element is encountered exceeds 0.5 after $\sqrt{N}$ choices have been made. Thus, for an m-bit hash value, if we pick data blocks at random, we can expect to find two data blocks with the same hash value within $k = \sqrt{2^m} = 2^{m/2}$ attempts.

(18) Alice and Bob share a secret key of some private key system. Bob has a message he claims came from Alice and to prove this, he produces a plaintext message and a ciphertext. The ciphertext decrypts to the plaintext under the secret key which Alice and Bo share. Please explain why this does not satisfy the requirements of non-repudiation of origin.

Ans: Non-repudiation refers to the ability to ensure that a party to a contract or a communication cannot refuse the authenticity of their signature on a document or that a message was actually sent.

Keeping this in mind, this fails the requirements of non-repudiation of origin because the cipher and plain texts can be obtained from the same key, held by both Alice and Bob. This has the probability of Bob creating his own plain text, encrypting it to create a corresponding cipher and claim to have received it from Alice (and vice versa). Since the truth in the claim be verified, this does not satisfy the requirements of non-repudiation of origin.

CRYPTOGRAPHY 106118105

Assignment - 2

19. Show that 64-bit message digest is vulnerable to collision attack. Assuming that adversary can perform 2^{20} tests (hash values) per second

Sol: Using birthday paradox,

for an m-bit hash value, if we pick data blocks at random, we can expect to find two data blocks with the same hash value within $k = \sqrt{2^m}$

$k = 2^{m/2}$ attempts

for 64-bit message

i.e., $m = 64$ collision occurs in $2^{64/2}$

i.e., 2^{32} attempts

If adversary can perform 2^{20} tests (hash values) per second, then it takes $\frac{2^{32}}{2^{20}}$ sec $= 2^{12}$ sec

$\Rightarrow$ The adversary takes 4096 sec to find collision which makes 64-bit message digest vulnerable to collision attack

20. What is the minimum and maximum number of padding bits that can be added to a message in SHA-512

Sol:- Minimum is 0. :

The minimum length of padding is 0 and it happens when $(-M-128) \bmod 1024$ is 0

$\Rightarrow |M| = -128 \bmod 1024$

$|M| = 896 \bmod 1024$ bits

In other words, the last block in the original message is 896 bits. We add a 128-bit length field to make the block complete.

Maximum is 1023. :

The maximum length of padding is 1023 and it happens when $(-|M|-128) = 1023 \bmod 1024$.

$\Rightarrow$ Length of the original message $|M| = (-128-1023) \bmod 1024$

$\Rightarrow |M| = 897 \bmod 1024$

In this case we cannot just add the length field because the length of the last block exceeds one bit more than 1024. So, we need to add 897 bits to complete this block and

create a second block of 896 bits.

Now the length can be added to make this block complete

21.25 Let $E : \{0,1\}^k \otimes B^n \rightarrow B^n$ be a block cipher, where $B = \{0,1\}^m$. View a message $M \in B^*$ as a sequence of l-bit blocks, $M = M[1] \ldots M[m]$. Consider $MAC : \{0,1\}^k \otimes B^* \rightarrow B$. Show that following MAC are forgeable under chosen message attack

- Function MAC is defined by $MAC_k(M[1] \cdots M[m]) = E_k(M[1]) \oplus \ldots \oplus E_k(M[m])$.

Sol:- Swapping any two messages blocks generates the same tag, hence knowing a (M,t) pair we can swap any two blocks in M to generate M' and pass (M', t) off as a forged valid MAC

∴ The given MAC is forgeable under chosen message attack

- Here $l = n - 32$. Function MAC is defined by $MAC_k(M[1] \ldots M[m]) = E_k(\langle 1 \rangle \| M[1]) \oplus \ldots E_k(\langle m \rangle \| M[m])$.

$\langle i \rangle$: is the 32-bit binary reperesantation of

the block index i.

Sol:

We have three chosen (M,T) pairs.

$E_k[M[1]||M[2]] = (1, M[1]) \oplus (2, M[2])$

$E_k[M[1]||M[1]] = (1, M[1]) \oplus (2, M[1])$

$E_k[M[2]||M[2]] = (1, M[2]) \oplus (2, M[2])$

Adding all 3 by XOR we get:

$E_k[M[2]||M[1]] = (1, M[2]) \oplus (2, M[1])$

∴ we successfully forged a valid tag for a new message.

22. To make the message multiple of block length n, padding is required. If padding is 00...00 then show that it may lead to some kind of forgery under CMA.

Sol:- Let us consider a case in which block size = N. The adversary selects 2 messages such that size of message 1 = m and message2 = m-1 and both the messages are same and the last

extra bit of message1 is 0.

By adding padding of 0* both the messages to be encrypted become same.

This leads to forgery.

For example

Consider, block size = 10

message 1 = 101010

message 2 = 10101

after padding,

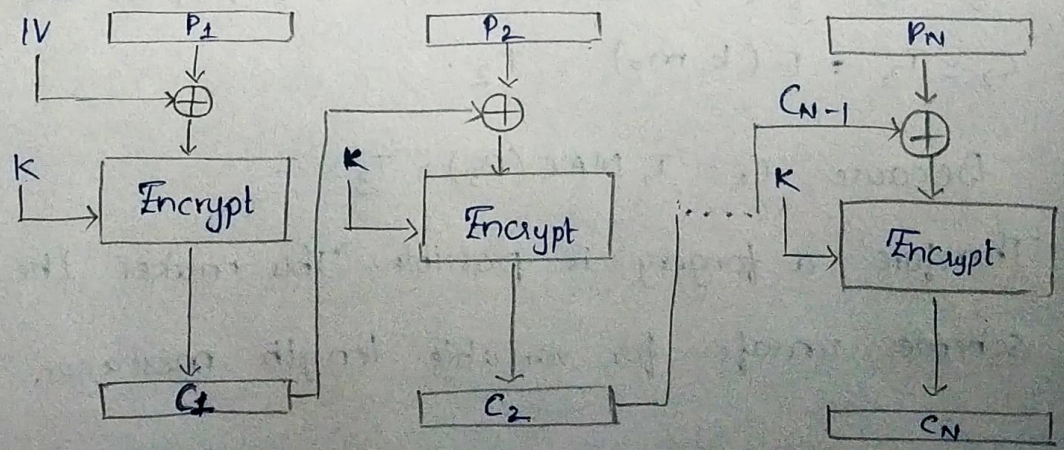
message 1 = 1010100000

message 2 = 1010100000

which can be used for forgery

23. If basic CBC-MAC is used for variable number of blocks then show that basic CBC-MAC is vulnerable for some kind of attack

Sol:-



The above figure shows CBC-MAC algorithm.

CBC-MAC is insecure for variable length messages.

Take two pairs of messages and tags (P_1, T_1) & (P_2, T_2), where $P_1 = m_0 \cdot m_1$ and $P_2 = m_0$.

Now, to forge the MAC tag, we ~~take~~ take another pair (P_3, T_3), where $(P_3 = m_0 \cdot m_1 \cdot (m_0 \text{ XOR } T_1))$ and $T_3 = T_2 \cdot \text{TakeIV}(00)$.

P_1 :

$C_0 = E(k, IV \oplus m_0)$

$T_1 = E(k, C_0 \oplus m_1)$

P_2 :

$T_2 = C_0 = E(k, IV \oplus m_0)$

P_3

$C_0 = E(k, IV \oplus m_0) = T_2$

$C_1 = E(k, C_0 \oplus m_1) = T_1$

$T_3 = C_2 = E(k, C_1 \oplus (m_0 \oplus T_1)) = E(k, C_1 \oplus m_0 \oplus T_1)$

$C_2 = T_3 = E(k, m_0) = T_2$.

Because $C_1 = T_1$ MAC $(P_3) = T_3$.

Therefore a forgery is possible. This makes the scheme unsafe for variable length messages.