Date:
Page No:

Q.8.

Ans. $\frac{1}{x} + \frac{1}{y} = \frac{1}{84}$

$$\frac{x+y}{xy} = \frac{1}{84}$$

$$xy - 84(x+y) = 0$$

$$(x-84)(y-84) = (84)^2$$

So $A \times B = (84)^2$

factors of $(84)^2 = 2^4 * 3^2 * 7^2$

So, possible Number of solutions from $2^4 \times 3^2 \times 7^2$

is $= (4+1)(2+1)(2+1)$

$= 5 \times 3 * 3 = 45$

Ans.

Date:
Page No:

Q.5

Ans.

31803221 is not a prime number.

given = $2^{31803212} \equiv 27696377 \pmod{31803221}$

$2^{31803212} \equiv 2^{31803221-9}$ or $\equiv 2^{n-9}$

By using Little fermat's theorem for any prime number p where $a \in Z_p$.

$a^{p-1} \equiv 1 \bmod p$

By multiplying both sides by 2^8.

$2^{n-9} \cdot 2^8 \equiv 27696377 \times 2^8 \equiv 29957450$

$\not\equiv 1 \bmod 31803221$

Hence, n is not a prime number

Date:
Page No:

Q.2.
Ans.

Given message size = 1000 characters. = N

$P(a) = 0.5$
$P(b) = 0.15$
$P(c) = 0.3$

$n = 4$

we know that

$$IC = \frac{\sum_{i=1}^{n} \binom{f_i}{2}}{N/2} = \frac{\sum f_i (f_i - 1)}{N(N-1)}$$

$$\Rightarrow \frac{1}{(N)(N-1)} \sum_{i=1}^{n} (f_i)(f_i - 1)$$

$$\frac{1}{(1000)(999)} \Big((0.5 \times 1000)(0.5 \times 1000 - 1) + (0.15 \times 1000)(0.15 \times 1000 - 1) + (0.3 \times 1000)(0.3 \times 1000 - 1) + (0.05 \times 1000)(0.005 \times 1000 - 1) \Big)$$

$$\frac{1}{1000 \times 999} = (500)(499) + (150 \times 149) + 300 \times (299) + 49 \times (50)$$

$$\frac{1}{1000 \times 999} (249500 + 22350 + 89700 + 2450)$$

Date:
Page No:

$$\Rightarrow \frac{364000}{999000} = 0.364$$

Q.9.

Ans. We know that $Z_3[x]/(x^3+cx^2+1)$ is a field if and only if the ideal generated by x^3+cx^2+1 is maximal ideal if and only if x^3+cx^2+1 is irreducible in $Z_3[x]$.

let $f(x) = x^3+cx^2+1$

Since $f(x)$ has degree 3., and if $f(x)$ is reducible then one of the factor should have degree one

i.e. $f(x)$ should have a root in Z_3

$f(0) = 0^3+c(0)^2+1 \equiv 1 \neq 0 \mod 3$

$f(1) = (1)^3+c(1)+1 = (2+c) \mod 3$

$f(2) = (8)+2c+1 = 9+c = c \mod 3$

So if $c \neq 0$ and $c \neq 1$ in Z_3, then $f(x)$ is irreducible

So, for $c \equiv 2$, $f(x)$ is irreducible.

Date:
Page No:

Q.1.

$p = 3 \cdot 2^n + 1$ n Natural number

let $n = 1 \Rightarrow 3 \cdot (2^1) + 1 = 7$

legendre symbol $\left(\frac{2}{7}\right) = 1$, so 2 is not a primitive root modulo 7.

let $n = 2 \Rightarrow 3(2^2) + 1 = 13$
and 2 is a primitive root modulo 13.

let $n > 3$.
Then $p = 3 \cdot 2^n + 1$

$\Rightarrow 8 \cdot 3 \cdot 2^{n-1} + 1$

So $p \equiv 1 \bmod 8$
This implies that $\left(\frac{2}{p}\right) = 1$.

Therefore 2 is a quadratic residue modulo p.
Hence 2 is not a primitive root modulo p.

Date:
Page No:

Q.4.

Ans. users A & B.

A's public keys (n, e)

B's public keys (n', e')

$n = pq \qquad n = pq'$

If a cryptanalyst somehow gets the values of n & n'.

Then he can find the gcd of n & n'

$x = \gcd(n, n')$

The gcd will be p as both p & q are prime numbers.

If p is found, then similarly q & q' can be found.

We know that

$\phi(n) = (p-1)(q-1)$

$\Rightarrow ed \equiv 1 \phi(n)$

$\Rightarrow d \equiv e^{-1} \phi(n)$

So both e & e' can be found. Hence private keys are found.

Date:
Page No:

Q.13.

Ans. Consider two Messages m_1 & m_2 using same random number k.

Now $r_1 = \alpha^k \bmod p$.

α – primitive root

$$t_1 = (\beta^k \cdot m_1) \bmod p$$

Now $(r_1, t_1) = (\alpha^k \bmod p, \beta^k m_1 \bmod p)$

Similarly for message 2.

$$r_2 = \alpha^k \bmod p$$

$$t_2 = (\beta^k \cdot m_2) \bmod p.$$

$$(r_2, t_2) = \alpha^k \bmod p, \beta^k m_2) \bmod p$$

let's compute

$$t_2 t_1^{-1} = \beta^k \cdot m_2 (\beta^k m_1)^{-1} \bmod p$$

$$\beta^k m_2 \beta^{-k} m_1^{-1} \bmod p$$

$$t_2 t_1^{-1} = (m_2 m_1^{-1}) \bmod p$$

Date:
Page No:

Now $M_2 = (t_2 t_1^{-1} \cdot m_1 \bmod p)$

If the attacker intercepts both the ciphertext & by chances discovers one plaintext m_1 then she can compute the other plaintext m_2.

Since both the plaintext are known, attacker can find the value of k.
and similarly find the value of private key: d.

Q.3.

Ans $n = 2k+1$

To prove $n \mid 2^{n!} - 1$

We know that n can be written as

$$n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$$

and $$\phi(n) = \prod_{i=1}^{r} p_i^{e_i - 1}(p_i - 1)$$

This number is a divisor of $n!$
Since each of its factors is $\leq n$ and they are all distinct.

Date:
Page No:

$S_0 = 2^{n!} = \left(2^{\phi(n)}\right)^{\frac{n!}{\phi(n)}} \equiv 1 \bmod n$

By Euler's theorem

So $2^{n!} - 1 \equiv 0 \bmod n$

or $n \mid (2^{n!} - 1)$.

Q.8.

Ans $E(F_{2^4}) : y^2 + y = x^3$

$P \in E(F_{2^4})$ is a point of order 3.

Let $P(x, y)$ be any point on E.

Using Koblitz curve mapping.

$F(x, y) = (x^{2^n}, y^{2^n})$ — (I)

Now $P(x, y)$

$-P(x, y+1)$ — (II)

$2P = (x^4, y^4 + 1)$ — (III)

Now $2P = -P$ (from (II) & (III))

Date:
Page No:

$= 3P = O$ i.e point of infinity

So order is 3.

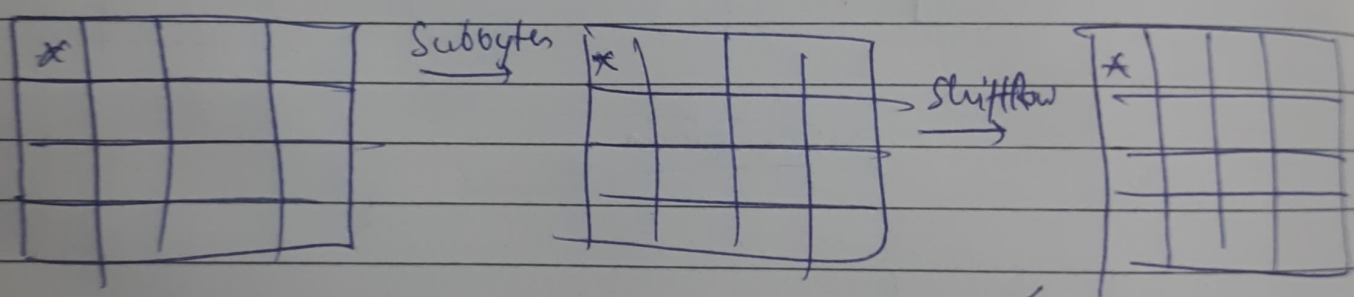
Date:
Page No:

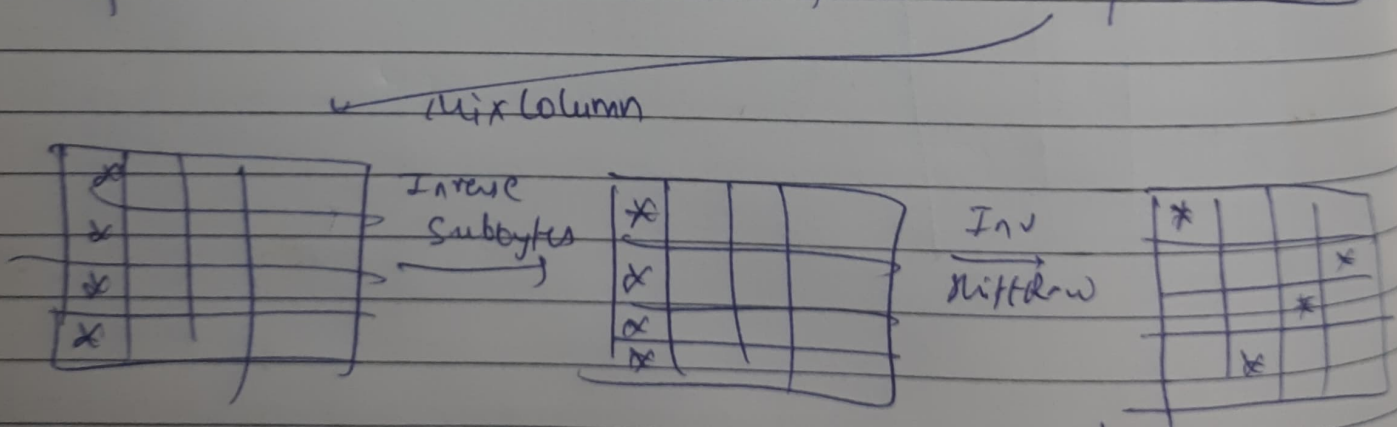
Q.12.

Ans. We know that shift Rows & Byte substitution are commutative.
While mix columns is not commutative.

Order I

1) SubBytes
2) ShiftRows
3) MixColumns



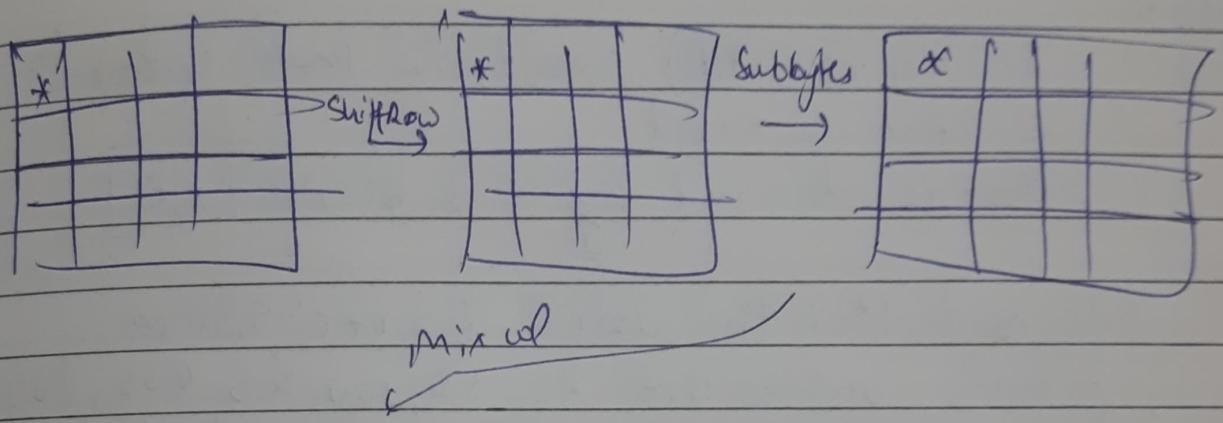


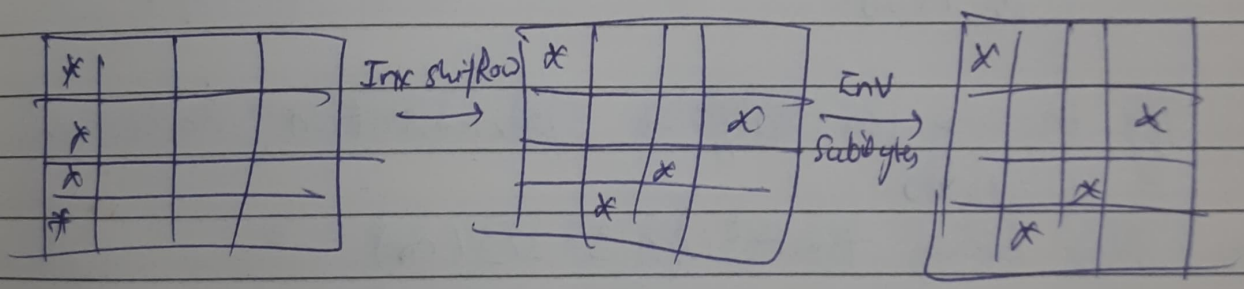
2nd MixColumn.

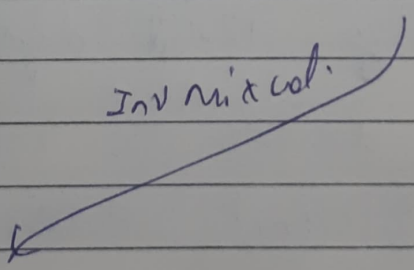
Date:
Page No:

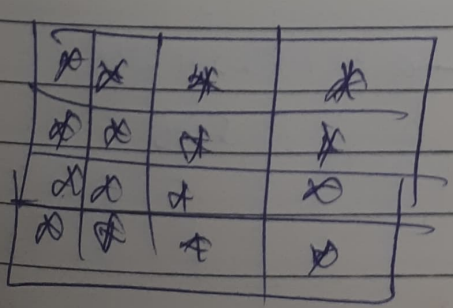
order 2

1) ShiftRow
2) Subbytes
3) MixColumn.









Date:
Page No:

Thus by changing Orders of shift Rows & Byte substitution result doesn't change

Q.10.

Ans. In SHA (KECCAK), we know that sponge function is used.
that is denoted by KECCAK [r,C]

We, now find the value b = r+C, whose possible values are 25, 50, 100, 200, 400, 800 or 1600.

By taking the largest permutation, we assume b = 1600

We Also know that SHA 3-512(m) constructing 512-bit digest

Therefore,
SHA-3-512(m) = C = 2×512 = 1024

r = 1600 − C = 1600 − 1024
= 576

Date:
Page No:

Now, we know that 3 cases are possible.

Case 1: $|m| = x * r$

Case 2: $|m| = x * r + q$ and $0 \leq q \leq r-2$

Case 3: $|m| = x * r + q$ and $q = r-1$

Given $|m| = 4000$

$4000 = 576 * 6 + 544$

Clearly, it is case 2.

Number of bits padded is

a 1 bit followed by $(r-q-2)$ 0 bits and last bit 1.

So, the Number of zero bits padded $= r - q - 2$

$= 576 - 544 - 2$

$= 30$

Ans = 30 bits

Date:
Page No:

Q.15 a) low degree LFSR are easily predictable because the sequences produced by them are periodic.

15. d) We know that Biometric is the alternate to maintain the privacy of key Using Biometric, we users protect from unauthorized access.
We can use a cryptographic key linked with users fingerprint data.
A string of binary numbers as cryptographic is extracted from fingerprint template (this key is used to encrypt a message.
Similarly for decryption we can use cryptographic key.

15. b) In BES only GF(2^8) is used
$= 2^{8} = 2^8$.

15. c) Symmetric Encryption we can use.
1) Traditional
2) Block
3) Hash
4) Stream

Date:
Page No:

1 Assymmetric Encryption:

a) Traditional
b) alternative.

15. a) Relinearization.

Q.14 (a) $h(m) = \alpha^m \bmod p$

In pre-image resistant: we know the value of $h(m)$. let's say β.

β known.

We know that discrete logarithmic problem is hard problem.
So it's preimage resistant & computationaly intractable.

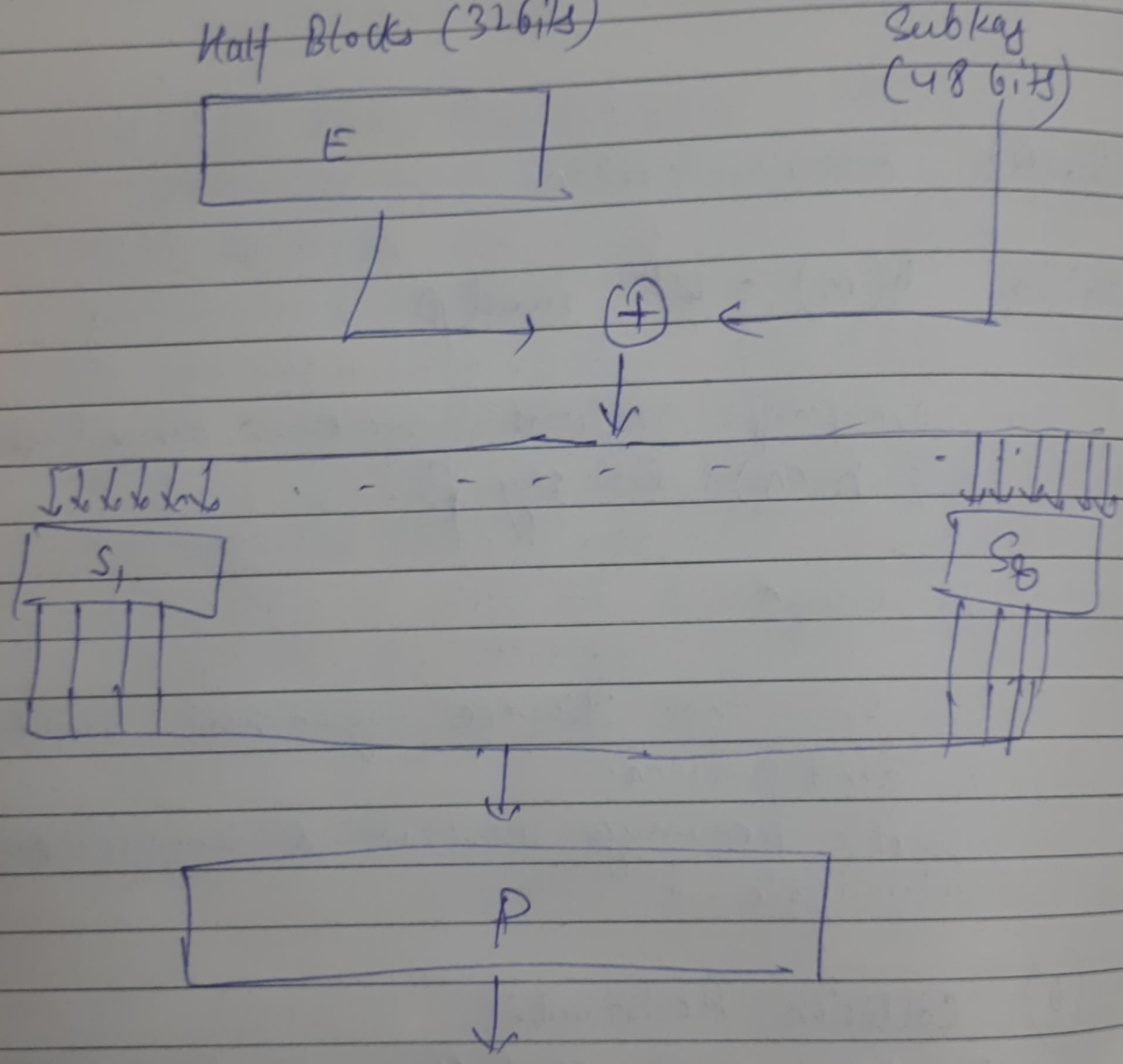
(b) Collision Resistant:
We know two m_1 & m_2 pair of messages with $h(m_1) = h(m_2)$

We know $m_1 \neq m_2$ The $\alpha^m \bmod p$ generate different values (or unique)
So $H(m_1) \neq H(m_2)$ So it's Collision Resistant.

Date:
Page No:

Q11.

Ans In DES



We can see that although the 8-S boxes are indeed compressing 48 bits down to 32, only 32 bits of entropy are coming from the original plaintext.
Therefore, we can get the remaining 16 bits

Date:
Page No:

from the key, when decrypting, which is the reason performed during reistad functions.

Date:
Page No:

Q7

$$m(x) = x^8 + x^4 + x^3 + x + 1$$

Find $f(x)$ such that

$$f(x) \cdot x \bmod m(x) = 1$$

$$x^8 + x^4 + x^3 + x + 1 \quad \text{--- (1)}$$

$$= (x^2+1)(x^6 + x^4 + x + 1) + x^2$$

$$x^6 + x^4 + x + 1 = (x^4 + x^2)(x^2) + x + 1$$

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

We will know express the remainder using eq. (1)

The below table contains coefficients such that $a(x)f(x) + b(x)g(x) = r(x)$:

$a(x)$	$b(x)$	$r(x)$
1	0	$x^8 + x^4 + x^3 + x + 1$
0	1	x
1	$x^3 + x^2 + 1$	$x^8 + 1$
1	$x^3 + x^3 + x^2 + 1$	1

Inverse is $x^7 + x^3 + x^2 + 1$

Date:
Page No:

Q.16

4 stage LFSR:

$C(x) = x^4 + x + 1$

$c_i = m_i \oplus s_{2i}$ for all $i, 1, 2 \ldots n$.

$m = m_1 m_2 \ldots \ldots m_7$

keystream = $S = s_1 s_2 s_3 \ldots$

ciphertext = 0 1 1 1 1 1 0

message = 1 1 1 1

keystream = 1 0 0 0

used

s_2 s_4 s_6 s_8