UNIT 2: Number theory:

- Divisibility & Division Algorithm
- Euclidian Algorithm
- modular arithmetic
- Prime numbers.

Finite Fields:

- Groups
- rings
- fields
- finite field of the form GF(p)
- polynomial arithmetic
- Finite fields of the form $GF(2^n)$

AES:

- AES transformation function
- AES key expansion
- AES example
- AES implementation

Block cipher operation:

- multiple encryption and triple DES
- ECB - CBC - CFB - OFB
- counter mode
- XTS AES Mode.

Divisibility Algorithm:

$b|a$ b is a divisor of a

A non zero b divides a, if $a = mb$ for some integer m where a, b, m are integers.

Properties:

1. If $a|1$, then $a = \pm 1$
2. If $a|b$ and $b|a$ then $a = \pm b$
3. If $a|b$ & $b|c$ then $a|c$ $a \to 11$ $b = 66$ $c = 198$

Division algorithm:

If we divide 'a' by 'n' we get an integer quotient q and integer remainder r

$$a = qn + r \qquad 0 \le r < n$$

Euclidian algorithm:

$GCD(a, b) = (b, a \bmod b)$ $8, 2 = 0$

$GCD(64, 24) = 16$ $64 > 2$ $2 \; 0 = 2$

(64 mod 24)

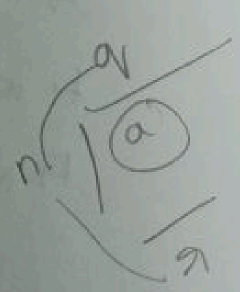
$GCD(24, 16)$

$GCD(16, 8)$

$GCD(8, 0) = 8$

$24 \overline{)64}$ (2) 48 16

$16 \overline{)24}$



① GCD (1970, 1066)
GCD (1066, 904)
GCD (904, 162)
GCD (162, 94)
GCD (94, 68)
GCD (68, 26)
GCD (26, 16)
GCD (16, 10)
GCD (10, 6)
GCD (6, 4)
GCD (4, 2)
GCD (2, 0) = 2

② GCD (24140, 16762)
GCD (16762, 7378)
GCD (7378, 2006)
GCD (2006, 1360)
GCD (1360, 646)
GCD (646, 68)
GCD (68, 34)
GCD (34, 0) = 34

Block cipher Modes:

① Electrical code Book Mode (ECB)
② Cipher Block chaining Mode (CBC)
③ Cipher FeedBack Mode (CFB)
④ Output FeedBack Mode (OFB)
⑤ counter Mode

Q	A	B	R
1	1970	1066	904
1	1066	904	162
	904	162	

⊙

Modulus operator

If a is a integer and n is a +ve integer we can define. a mod n to be the remainder when a is ÷ by n.

$$a = qn + r \qquad 0 \le r < n$$

congruent:

two integers a and b are said to be congruent modulo n.

$\Rightarrow a \equiv b \bmod n$

$\Rightarrow a \bmod n = b \bmod n$

Properties of congruent:

* $a \equiv b \bmod n$ if $n \mid (a-b)$

eg: $23 \equiv 8 \bmod 5$

$5 \mid (23-8)$

$5 \mid 15$ 5 is a divisor of 15

* $a \equiv b \bmod n$ implies $b \equiv a \bmod n$

* $a \equiv b \bmod n$ and $b \equiv c \bmod n$

implies $a \equiv c \bmod n$.

Properties

① [a m

② [a m

③ [a m

eg: a =

① =>

Modula

1, 11

Sol

11 mo

Properties of Modular Arithmetic :

① $[a \bmod n + b \bmod n] \bmod n = (a+b) \bmod n$

② $[a \bmod n - b \bmod n] \bmod n = (a-b) \bmod n$

③ $[a \bmod n * b \bmod n] \bmod n = (a*b) \bmod n$.

eg: $a = 11, \; b = 15, \; n = 8$

① $\Rightarrow [11 \bmod 8 + 15 \bmod 8] \bmod 8 = (11+15) \bmod 8$

$[3 + 7] \bmod 8 = 26 \bmod 8$

$2 = 2$

Modular Exponentiation :

1, $11^7 \bmod 13$

Sol $11^2 \bmod 13 = 121 \bmod 13 = 4$

$11^4 \bmod 13 = [(11^2 \bmod 13)(11^2 \bmod 13)] \bmod 13$

$= [4 * 4] \bmod 13$

$= 3$

$11^7 \bmod 13 = [(11^4 \bmod 13)(11^2 \bmod 13)(11^1 \bmod 13)] \bmod 13$

$= [3 \times 4 \times 11] \bmod 13$

$= 132 \bmod 13$

$= 2$

2. $19^{25} \bmod 17$

$19^2 \bmod 17 = 361 \bmod 17 = 4$

$19^5 \bmod 17 = [(19^2 \bmod 17)(19^2 \bmod 17)(19 \bmod 17)] \bmod 17$

$= [4 * 4 \times 2] \bmod 17$

$= 32 \bmod 17$

$= 15$

$19^{25} \bmod 17 = [(19^5 \bmod 17)(19^5 \bmod 17)(19^5 \bmod 17)$
$(19^5 \bmod 17)(19^5 \bmod 17)] \bmod 17$

$= [15 \times 15 \times 15 \times 15 \times 15] \bmod 17$

$= 759,375 \bmod 17$

$= 8.$

Define the set Z_n as the set of non negative integers $< n$. $Z_n = \{0, \ldots (n-1)\}$

$Z_5 = \{0, 1, 2, 3, 4\}$

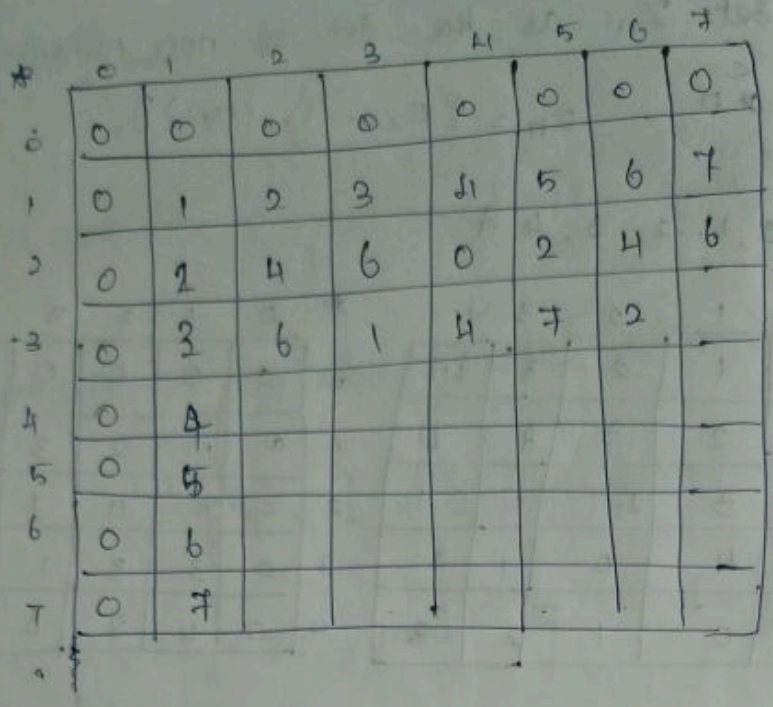
+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

*	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	3	1	4
4	0	4	3	2	1

a	-a	a'
0	0	-
1	4	1
2	3	3
3	2	2
4	1	4

$Z_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6



*	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	
4	0	4						
5	0	5						
6	0	6						
7	0	7						

Relatively Prime:

Two integers are relatively prime if there only common integer factor is one.

Euler's totient function [$\phi(n)$]

→ product of 2 prime nos

Number of +ve integers less than n and relatively prime to n

$n = p \times q$

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

eg: $p = 3$, $q = 5$, $n = 3 \times 5 = 15$

$\phi(15) = (2) * (4) = 8$

$= \{1, 2, 4, 7, 8, 11, 13, 14\}$ are relatively prime

→ doesn't contain p and q value and also multiples of p & q.

① → 1st factor the n we get $p, p_1, \ldots$

② → $\phi(n) = n\left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{q}\right)$

Group:

A Group G is a set of elements denoted by binary operation • , that satisfies four properties or four axioms ~~(A1)~~ as

(A_1) closure : if $a, b \in G$, then $a \cdot b \in G$

(A_2) Associative : if $a, b, c \in G$ then $a.(b.c) = (a.b).c$

(A_3) Identity (e): If $e \in G$, then $e.a = a.e = a$

(A_4) Inverse (a^{-1}) : If $a' \in G$, then $a.a' = a'.a = e$

N_n is the set with 'n' different symbols

S_n is the set of all permutations of 'n' different symbols.

eg: $n = 3$

$N_n = \{1, 2, 3\}$

$S_n = \{\{1,2,3\}, \{1,3,2\}, \{2,1,3\}, \{2,3,1\}, \{3,1,2\}, \{3,2,1\}\}$

Note: for n no. of. sets we have $n!$ combinations.

for closure:

let $a = \{1,3,2\}$ $b = \{3,1,2\}$

$A1 : a.b = \{1,3,2\} . \{3,1,2\}$

$= \{3,2,1\} \in G$

for associative :

$a = \{1, 3, 2\}$ $b = \{3, 1, 2\}$ $c = \{2, 1, 3\}$

LHS $\Rightarrow$ $a.(b.c) = a.(\{3, 1, 2\} . \{2, 1, 3\})$
$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad 1\ 2\ 3$

$= a.(\{3, 2, 1\})$

$= \{1, 3, 2\} . \{3, 2, 1\}$

$= \{3, 1, 2\}$

RHS $\Rightarrow$ $(a.b).c = (\{1, 3, 2\} . \{3, 1, 2\}) . \{2, 1, 3\}$

$= \{3, 2, 1\} . \{2, 1, 3\}$

$= \{3, 1, 2\}$

for identity :

Identity mapping is the permutation that doesnot alter the order of n elements

A3 : Identity $\Rightarrow$ $a.e = e.a = a$

LHS $\{1, 3, 2\} . \{1, 2, 3\} = \{1, 3, 2\} = a$

RHS $\{1, 2, 3\} . \{1, 3, 2\} = \{1, 3, 2\} = a$

for inverse :

AH : $a \cdot a^{-1} = a^{-1} \cdot a = e$

$a = \{1, 3, 2\}$ $a^{-1} = \{1, 3, 2\}$

$a \cdot a^{-1} = \{1, 3, 2\} \cdot \{1, 3, 2\} = \{1, 2, 3\} = e$

$a^{-1} \cdot a = \{1, 3, 2\} \cdot \{1, 3, 2\} = \{1, 2, 3\} = e$

$\therefore S_3$ is a Group.

(AF) : Commutative :

If $a, b \in G$ then $a \cdot b = b \cdot a$

$a = \{1, 3, 2\}$ $b = \{3, 1, 2\}$

$a \cdot b = \{3, 2, 1\}$

$b \cdot a = \{3, 1, 2\} \cdot \{1, 3, 2\}$

$= \{2, 1, 3\}$

LHS $\neq$ RHS

If a group G satisfies all the properties A1 to A5 then G is said to be an Abelian group.

Problem: For the group S_n of all permutations of n distinct symbols.

(i) what is no. of. elements in S_n

(ii) show that S_n is abelian group for $n \leq 3$

$n=2$

$N_2 = \{1, 2\}$

$S_2 = \{\{1, 2\}, \{2, 1\}\}$

A1 : $a = \{1, 2\}$ $b = \{2, 1\}$

$a \cdot b = \{2, 1\} \in S_2$

A2 : $a = \{1, 2\}$ $b = \{2, 1\}$ $c = \{1, 2\}$

$a \cdot (b \cdot c) = a \cdot (\{2, 1\} \cdot \{1, 2\})$

$= a \cdot \{2, 1\}$

$= \{2, 1\}$

$(a \cdot b) \cdot c = \{2, 1\} \cdot \{1, 2\}$

$= \{2, 1\}$

LHS = RHS

A3 : $a \cdot e = \{1, 2\} \cdot \{1, 2\} = \{1, 2\} = a$

$e \cdot a = \{1, 2\} \cdot \{1, 2\} = \{1, 2\} = a$

A4 : $a = \{1,2\}$ $a' = \{1,2\}$

$a \cdot a' = \{1,2\} \cdot \{1,2\} = \{1,2\} = e$

$a' \cdot a = \{1,2\} \cdot \{1,2\} = \{1,2\} = e$

$\therefore$ it is a group

A5 :

$a \cdot b = b \cdot a$

$\{1,2\} \cdot \{2,1\} = \{2,1\} \cdot \{1,2\}$

$\{2,1\} = \{2,1\}$

$\therefore$ the group S_2 is abelian group.

Note : * If a group has a finite no. of. elements then it is refered as finite group ~~then it~~.

* Order of the group = No. of. elements in the group.

Ring :

a Ring R is denoted $\{R, +, * \}$ is a set of elements with two binary operations called addition and multiplications such that for all a, b, c in R.

① $(A_1 - A_5)$ with +

② (M1) : closure under multiplication

If $a, b \in R$ then $a * b \in R$

(M2) : Associativity of multiplication.

If $a, b, c \in R$ then $a*(b*c) = (a*b)*c$

(M3) distributive :

$$a(b+c) = ab + ac$$

$$(a+b)c = ac + bc$$

, $a, b, c \in R$

(M4) commutative Ring :

$$a * b = b * a \quad , \quad a, b \in R$$

(M5) multiplicative identity :

$$1 * a = a * 1 = a \quad , \quad a \in R$$

(M6) No zero Divisors :

If a and b $\in R$ and $ab = 0$

then either $a = 0$ or $b = 0$.

If R satisfies A_1 to A_5 with + and M_1 to M_3 then it is a Ring.

example :

Z_n = {0,

Z_5 = {0,

let a =

A1 : a+b

A2 : a+(b

1+

A3 : a+

1+

A4 : a+b

A5 : a+

1+

8

M1 : a

M2 :

example:

Z_n : {0, ... (n-1)} → residue class modulo n.

Z_5 : {0, 1, 2, 3, 4}

let a = 1 b = 2 c = 3

A1 : $a+b = 1+2 \bmod 5 = 3 \in Z_5$

A2 : $a+(b+c) = (a+b)+c$

$1+(2+3) = (1+2)+3$

$6 = 6$

$1 = 1$ & so $\in Z_5$

A3 : $a+e = e+a = a$; $e = 0$

$1+0 = 0+1 = 1 \Rightarrow a$

AH : ~~a+b~~ $= a+(-a) = (-a)+a = e$

$1+(-1) = (-1)+a = 0 \Rightarrow e$

A5 : $a+b = b+a$

$1+2 = 2+1$

$3 = 3 \in Z_5$

M1 : $a*b \in Z_5$

$1*2 \in Z_5$

$2 \overset{\text{mod } 5}{\in} Z_5$

M2 : $a*(b*c) = (a*b)*c$

$1*(2*3) = (1*2)*3$

$6 = 6$

$1 = 1 \in Z_5$

$a(b+c) = ab+ac$

M_8: $1(2+3) = 1*2 + 1*3$

$5 = 2+3$

$5 = 5$

$0 = 0$

$(a+b)c = ac+bc$

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

$9 = 9$

M_{11}: $a*b = b*a$

$1*2 = 2*1$

$2 = 2$

M_9: $1*a = a*1 = a$

$1*1 = 1*1 = 1 = a$

Note:

* If $A_1 - A_{11}$ satisfied then its Group
* If $A_1 - A_5$ satisfied then its Abelian group
* If $A_1 - A_5 + M_1 - M_{11}$ satisfied then its Abelian ring
* If $A_1 - A_5 + M_1 - M_6$ satisfied then it is Ring.

Field (F)

is a set

called a

for

(M7) M

element

Z_4 :

*	0
0	0
1	0
2	0
3	0

Field (F)

the field (F) is denoted by {F, +, *}

is a set of elements with 2 binary operations called addition & multiplication

for all $a, b, c \in F$.

(M7) Multiplicative Inverse

for each $a \in F$, except 0 there is an element $a^{-1} \in F$, such that

$$aa^{-1} = a^{-1}a = 1$$

$Z_4 = \{0, 1, 2, 3\}$

*	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	3

a	a^{-1}
0	-
1	1
2	-
3	3

$Z_5 = \{0, 1, 2, 3, 4\}$

*	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

a	a^{-1}
0	-
1	1
2	3
3	2
4	4

Polynomial Arithmetic:

① ordinary polynomial arithmetic. ×

② polynomial arithmetic over GF(p) → prime no

③ polynomial arithmetic over GF(p^n)

$$f(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \dots + a_1 x + a_0$$

$$f(x) = \sum_{i=0}^{n-1} a_i x^i$$

constant polynomial:

A zero degree polynomial is called constant polynomial

Monic polynomial

An n^{th} degree polynomial is said to be monic polynomial

(I)

$$f(x) = x^3 + x^2 + 2$$

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

$$f(x) + g(x) = \begin{array}{r} x^3 + x^2 + 2 \\ x^2 - x + 1 \\ \hline x^3 + 2x^2 - x + 3 \end{array}$$

$f(x) - g(x) = x^3 + x + 1$

$f(x) * g(x) = x^5 + x^4 + x^3 + x^4 - x^3 + x^2$

$+ 2x^2 - 2x + 2$

$= x^5 + 3x^2 - 2x + 2$

$f(x) / g(x) =$

$q(x) = (x + 2)$

$r(x) = x$

$f(x) = q(x) g(x) + r(x)$

If GF(2)

$Z_2 = \{0, 1\}$

$f(x) = x^7 + x^5 + x^4 + x^3 + x + 1$

$g(x) = (+) \quad + x^3 + x + 1$ (2 x^3 mod 2)

$x^7 + x^5 + x^4$

$f(x) - g(x) = x^7 + x^5 + x^4 + x^3 + x + 1$

$x^3 + x + 1$

$x^7 + x^5 + x^4$

$f(x) * g(x) = (x^7 + x^5 + x^4 + x^3 + x + 1)(x^3 + x + 1)$

$= x^{10} + x^8 + x^6 + x^4 + x^3$

$x^8 + x^6 + x^5 + x^4 + x^2 + x$

$x^7 + x^5 + x^4 + x^3 + x + 1$

$= x^{10} + x^4 + x^2 + 1$

$$
\begin{array}{r|l}
x^3 + x + 1 & x^4 + 1 \\
\hline
x^7 + x^5 + x^4 + x^3 + x + 1 & \\
x^7 + x^5 + x^4 & \\
\hline
x^3 + x + 1 & \\
x^3 + x + 1 & \\
\hline
0 &
\end{array}
$$

GCD(a(x), b(x)) = GCD(b(x), a(x) mod b(x))

Prob $a(x) = x^4 + x^2 + x + 1$

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

find gcd over $gf(2)$

Sol

$$
\begin{array}{r|l}
x^3 + x^2 + 1 & x + 1 \\
\hline
x^4 + x^2 + x + 1 & \\
x^4 + x^3 + x & \\
\hline
x^3 + x^2 + 1 & \\
x^3 + x^2 + 1 & \\
\hline
0 &
\end{array}
$$

GCD $(x^4 + x^2 + x + 1, x^3 + x^2 + 1)$

GCD $(x^3 + x^2 + 1, 0)$

GCD $= x^3 + x^2 + 1$

prob

gf. $a(x) = x^4 + x^3 + x$

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

find gf(2)

sol

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

$x^4 + x^2$

$x^3 + x^2 + x$

$x^3 + x$

x^2

$x^2 + 1$

1

GCD $(x^4+x^3+x,\ x^2+1)$

GCD $(x^2+1,\ x^2+x+1)$

GCD $(x^2+1,\ 1)$

GCD $(1, 0)$

GCD $= 1$

prob

$a(x) = 5x^2 + 3x + 9$

$b(x) = 4x^3 + 15$

perform multiplication over GF(17)

$20x^5 + 45x^2$

$+45x$

$12x^4$

$+36x^3$

$+135$

mod 17

$3x^5 + 18x^4 + 2x^3 + 7x^2 + 11x + 16$

Polynomial Arithmetic over GF(p^n)

$$f(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \dots + a_1 x + a_0$$

$$f(x) = \sum_{i=0}^{n-1} a_i x^i$$

$$f(x) = a_1 x^1 + a_0 = a_1 x + a_0$$

$$\boxed{f(x) = a_1 x + a_0}$$

$GF(2^2) \Rightarrow p^n = 2^2 = 4$ → ($n = 2$, $p = 2$)

$Z_p = \{0, 1\}$

$a_1\ a_0$	
00	$\Rightarrow f(x) = 0x + 0 = 0$
01	$\Rightarrow 0x + 1 = 1$
10	$\Rightarrow 1x + 0 = x$
11	$\Rightarrow 1x + 1 = x + 1$

$GF(2^2) = 4$ polynomials

$0, 1, x, x+1$

+	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

w	$-w$
0	0
1	1
x	x
$x+1$	$x+1$

$GF(2^3)$, $p = 2$, $n = 3$ $\Rightarrow$ $p^n = 2^3 = 8$ polynomials

$Z_p = \{0, 1\}$

$000 \Rightarrow f(x) = a_2x^2 + a_1x + a_0 = 0$

$001 \rightarrow 1$

$010 \Rightarrow x$

$011 \Rightarrow x + 1$

$100 \Rightarrow x^2$

$101 \Rightarrow x^2 + 1$

$110 \Rightarrow x^2 + x$

$111 \Rightarrow x^2 + x + 1$

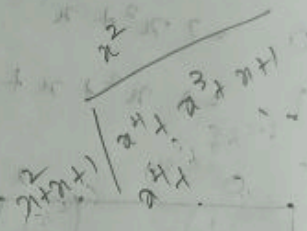
+	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
1	1	0	$x+1$	x	x^2+1	x^2	x^2+x+1	x^2+x
x	x	$x+1$	0	1	x^2+x	x^2+x+1	x^2	x^2+1
$x+1$	$x+1$	x	1	0	x^2+x+1	x^2+x	x^2+1	x^2
x^2	x^2	x^2+1	x^2+x	x^2+x+1	0	1	x	$x+1$
x^2+1	x^2+1	x^2	x^2+x+1	x^2+x	1	0	$x+1$	x
x^2+x	x^2+x	x^2+x+1	x^2	x^2+1	x	$x+1$	0	1
x^2+x+1	x^2+x+1	x^2+x	x^2+1	x^2	$x+1$	x	1	0

w	$-w \Rightarrow$
0	0
1	1
x	x
$x+1$	$x+1$
x^2	x^2
x^2+1	x^2+1
x^2+x	x^2+x
x^2+x+1	x^2+x+1

2, $GF(3^2)$, $p=3$, $n=2$ $p^n = 3^2 = 9$ polynomials

$Z_p = \{0, 1, 2\}$

a_1	a_0	
0	0	0
0	1	1
0	2	2
1	0	x
1	1	$x+1$
1	2	$x+2$
2	0	$2x+0$
2	1	$2x+1$
2	2	$2x+2$



Irreducible Polynomial / Prime polynomial :

A polynomial $f(x)$ over a field F is called irreducible if and only if, $f(x)$ cannot be expressed as a product of two polynomials and both of the degree lower than that of $f(x)$.

It is denoted by $m(x)$

eg:

$x^3 + x + 1$

$x^8 + x^4 + x^3 + x + 1$

polynomial

Prob find multiplicative inverse of x^2+x+1 with $m(x) = x^3+x+1$ over $GF(2^3)$

$p=2$ $n=3$, $p^n = 2^3 = 8$ polynomial.

Q	A	B	R	t_1	t_2	t
	x^3+x+1	x^2+x+1				
$x+1$	x^3+x+1	x^2+x+1	x	0	1	$-x-1$
x^2+1	x^2+x+1	x	1	1	$-x-1$	x^3+x^2+x+2
x	x	1	0	$-x-1$	x^3+x^2+x+2	
-	1	0	-			

Prob

Q	A_1	A_2	A_3	B_1	B_2	B_3
-	1	0	x^3+x+1	0	1	x^2+x+1
$x+1$	0	1	x^2+x+1	1	$x+1$	x
$x+1$	1	$x+1$	x	$x+1$	x^2	1

MI

Prob: (x^7+x+1) with $m(x) = x^8+x^4+x^3+x+1$ over $gf(2^8)$. find MI

x^7+x+1

AES algorithm

Mix column

$$\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} 87 \\ 6E \\ 46 \\ A6 \end{pmatrix}$$

$02 * 87 \oplus 03 * 6E \oplus 01 * 46 \oplus 01 * A6$

↓

$(0000\ 0010) * (1000\ 0111)$

$x^1 * (x^7 + x^2 + x + 1)$

$= x^8 + x^3 + x^2 + x \mod (x^8 + x^4 + x^3 + x + 1)$

M(x)

Problem:

Given the plain text, 00010203040506070809 0A0B0C0D0E0F and the key 0101010101010101010101010101

(i) Show the original contents of state displayed as 4×4 matrix.

(ii) Show the value of state after initial add round key

(iii) " " " " " substitute bytes

(iv) " " " " shift rows

(v) " " " " mixed column.

(i)

00	
01	
02	
03	

(ii)

00	
01	
02	
03	

(iii)

(iv) Shi

(i)

00	04	08	0C
01	05	09	0D
02	06	0A	0E
03	07	0B	0F

(ii)

00	04	08	0C
01	05	09	0D
02	06	0A	0E
03	07	0B	0F

⊕

01	01	01	01
01	01	01	01
01	01	01	01
01	01	01	01

⇓

01	05	09	0D
00	04	08	0C
03	07	0B	0F
02	06	0A	0E

0000 0101
0000 0001
0000 0100

(iii)

01	05	09	0D
00	04	08	0C
03	07	0B	0F
02	06	0A	0E

sbox =>

7C	6B	01	D7
63	F2	30	FE
7B	C5	2B	76
77	6F	67	AB

(iv) shift rows

7C	6B	01	D7
F2	30	FE	63
2B	76	7B	C5
AB	77	6F	67

=> 0 shift
=> 1 shift
=> 2 shift
=> 3 shift

v) mixed column :

$$\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} 7C \\ F2 \\ 2B \\ AB \end{pmatrix} = \begin{pmatrix} 75 \\ 55 \\ \\ \end{pmatrix}$$

$02 * 7C \Rightarrow 0000\ 0010 * 0111\ 1100$

$= x * (x^6 + x^5 + x^4 + x^3 + x^2)$

$= x^7 + x^6 + x^5 + x^4 + x^3$

$= \boxed{1111\ 1000}$ (+)

$03 * F2 \Rightarrow 0000\ 0011 * 1111\ 0010$

$= (x+1) * (x^7 + x^6 + x^5 + x^4 + x)$

$= x^8 + x^7 + x^6 + x^5 + x^2 + x^7 + x^6 + x^5 + x^4 + x$

$= x^8 + x^4 + x^2 + x \mod x^8 + x^4 + x^3 + x + 1$

$= x^3 + x^2 + 1$

$= \boxed{0000\ 1101}$ (+)

$01 * 2B = \boxed{0010\ 1011}$ (+)

$01 * AB = \boxed{1010\ 1011}$ (+)

$02 * 7C \Rightarrow 1111\ 1000$

$03 * F2 \Rightarrow 0000\ 1101$

$01 * 2B \Rightarrow 0010\ 1011$

$01 * AB \Rightarrow 1010\ 1011$ (+)

$0111\ 0101 \Rightarrow 75$

$01 * 7C =$

$02 * F2 =$

$03 * 2B =$

$04 * AB =$

$01 * 7C =$

$01 * F2$

$02 * 2B$

$03 * AB$

01 * 7C = 0111 1100
02 * F2 = 1111 1111
03 * 0B = 0111 1101
04 * AB = 1010 1011 ⊕
0101 0101 => 55

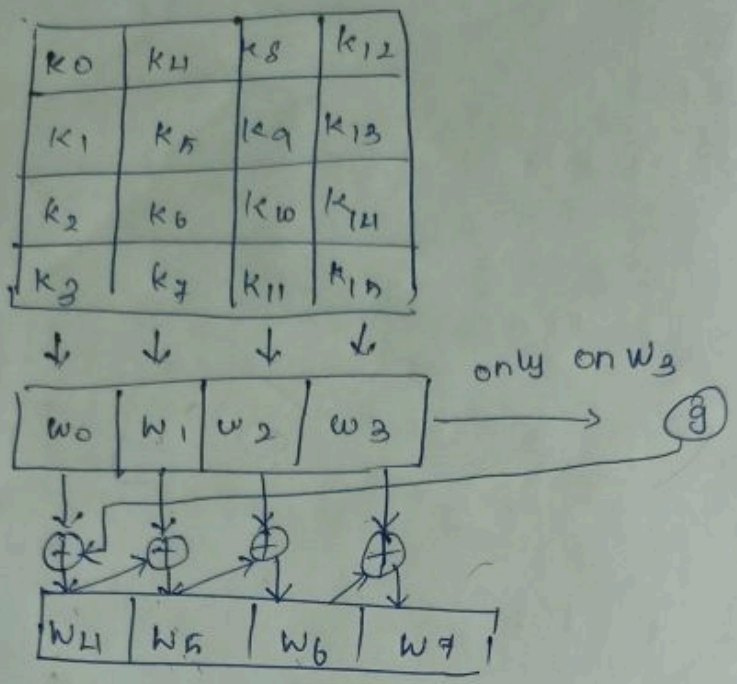
01 * 7C = 0111 1100

01 * F2 = 0000 0001 * 1111 0010
= 1 * ($x^7 + x^6 + x^5 + x^4 + x$)
= 1111 0010

02 * 2B = 0000 0010 * 0010 1011
= x * ($x^5 + x^3 + x + 1$)
= $x^6 + x^4 + x^2 + x$
= 01010110

03 * AB = 0000 0011 * 1010 1011
= ($x+1$) * ($x^7 + x^5 + x^3 + x + 1$)
= $x^8 + x^6 + x^4 + x^2 + x + x^7 + x^5 + x^3 + x + 1$
= $x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + 1$
= $x^7 + x^6 + x^5 + x^2$
= 1110 0100

AES key expansion:



Problem: 54, 68, 61, 74, 73, 20, 6D, 79, 20, 48, 75, 6E, 67, 20, 46, 75 Generate W_4 to W_7 (round = 7)

Apply 'g' operation on w[3]

① Apply circular byte left shift

② Apply byte substitution

③ Add round constant

i	1	2	3	4	5	6	7	8	9	10
RC_i	01	02	04	08	10	20	40	80	1B	36

Key: { 54 68 61 74 73 20 6D 79 20
4B 75 6E 67 20 46 75 }

54	73	20	67
68	20	4B	20
61	6D	75	46
74	79	6E	75

w[0] w[1] w[2] w[3]

w[0] = { 54, 68, 61, 74 }

w[1] = { 73, 20 6D 79 }

w[2] = { 20 4B, 75 6E }

w[3] = { 67 20 46 75 }

g[w[3]] = { 67 20 46 75 }

① → { 20 46 75 67 }

② → { B7 5A 9D 85 }

③ → B7 5A 9D 85

④ 01 00 00 00

B6 5A 9D 85

g[w[3]] = B6 5A 9D 85

w[4] = w[0] ⊕ g[w[3]]

0100 0000

1011 0111

0000 0001

1011 0110

B 6

$w[0]$: 01010100 (54) 01101000 (68) 01100001 (61) 01110100 (74)

$g(w[3])$: 10110110 (B6) 01011010 (5A) 10011101 (9D) 10000101 (85)

⊕

$w[4]$: 11100010 (E2) 00110010 (32) 11111100 (FC) 11110001 (F1)

$w[5] = w[4] \oplus w[1]$

$w[4]$: 1110 0010 (E2) 0011 0010 (32) 1111 1100 (FC) 1111 0001 (F1)

$w[1]$: 73 (0111 0011) 20 (0010 0000) 6D (0110 1101) 79 (0111 1001)

1001 0001 (91) 0001 0010 (12) 1001 0001 (91) 1000 1000 (88)

$w[5]$: 91 12 91 88

$w[6] = w[5] \oplus w[2]$

$w[5]$: 1001 0001 (91) 0001 0010 (12) 1001 0001 (91) 1000 1000 (88)

$w[2]$: 0010 0000 (20) 0100 1011 (4B) 0111 0101 (75) 0110 1110 (6E)

1011 0001 (B1) 0101 1001 (59) 1110 0100 (E4) 1110 0110 (E6)

$w[6]$: B1 59 E4 E6

$w[7] = w[6] \oplus w[3]$

$w[6]$: B1 59 E4 E6

$w[3]$: 67 (0110 0111) 20 (0010 0000) 46 (0100 0110) 75 (0111 0101)

1101 0110 (D6) 0111 1001 (79) 1010 0010 (A2) 1001 0011 (93)

$w[7]$: D6 79 A2 93

---

construction

$$\begin{bmatrix} b0' \\ b1' \\ b2' \\ b3' \\ b4' \\ b5' \\ b6' \\ b7' \end{bmatrix} =$$

eg :

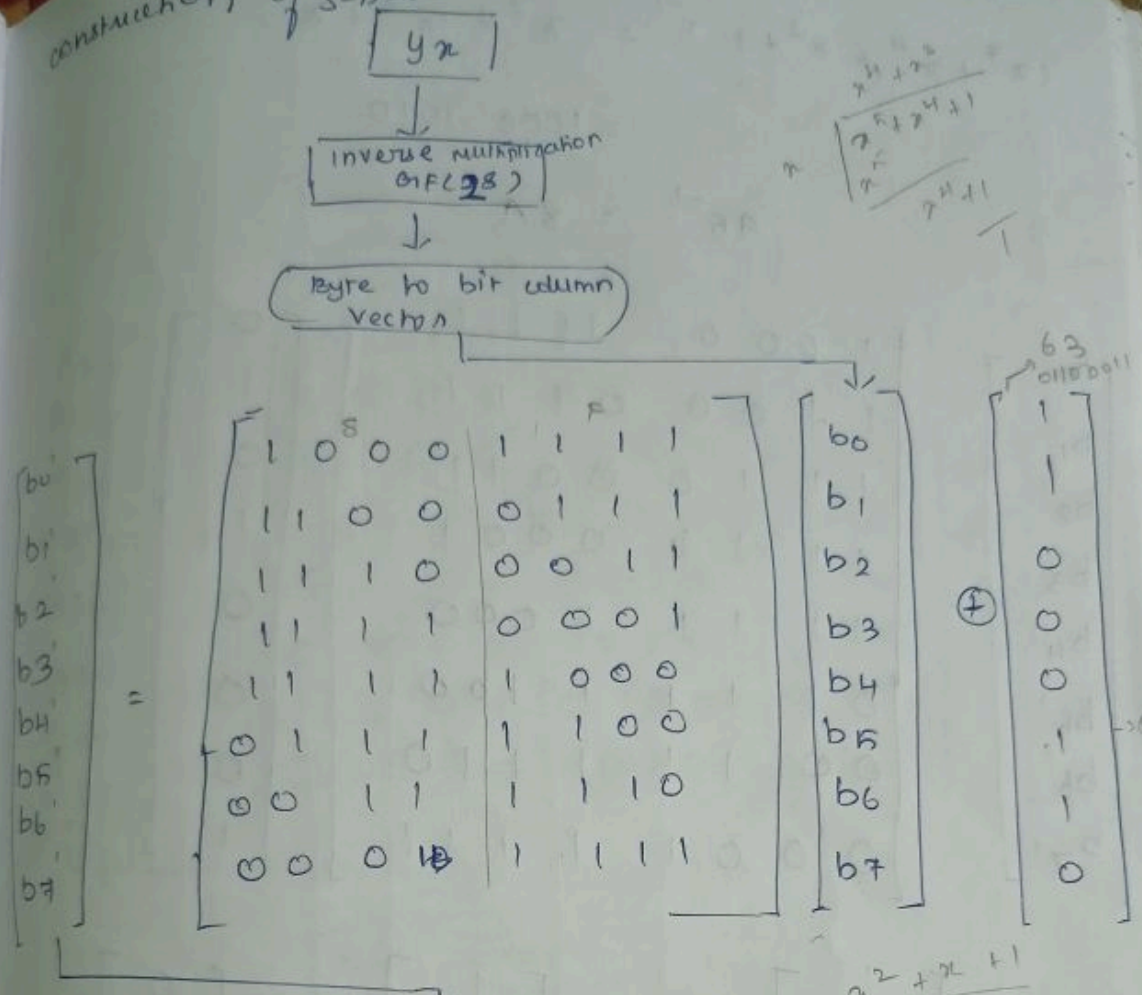
Q

x

x^2+x+1

x^4+x^3

construction of s-box:



eg: $a_5 \Rightarrow a_5^{-1} \Rightarrow (10010101)^{-1} \rightarrow (x^7 + x^4 + x^2 + 1)$

mod $(x^8 + x^4 + x^3 + x + 1)$

Q	A_1	A_2	A_3	B_1	B_2	B_3
–	1	0	$x^8 + x^4 + x^3 + x + 1$	0	1	$x^7 + x^4 + x^2 + 1$
x	0	1	$x^7 + x^4 + x^2 + 1$	1	x	$x^5 + x^4 + 1$
$x^2 + x + 1$	1	x	$x^5 + x^4 + 1$	$x^2 + x + 1$	$x^3 + x^2 + x + 1$	x
$x^4 + x^3$	$x^2 + x + 1$	$x^3 + x^2 + x + 1$	x	$x^6 + x^3 + 1$	$x^7 + x^3 + x$	1

$(x^7 + x^4 + x^2 + 1)^{-1} = x^7 + x^3 + x$

$= 1000\ 1010$
$\quad b_7 \qquad b_0$

$95^{-1} = 8A$

$$\begin{bmatrix} b_0' \\ b_1' \\ b_2' \\ b_3' \\ b_4' \\ b_5' \\ b_6' \\ b_7' \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \times \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \oplus 1 \\ 1 \oplus 1 \\ 1 \oplus 1 \oplus 1 \\ 1 \oplus 1 \\ 1 \oplus 1 \\ 1 \\ 1 \oplus 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} \Rightarrow \oplus \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

formula

$= 00101010$

$= 2A$

$95^{-1} \rightarrow 8A \rightarrow 2A$

construction of

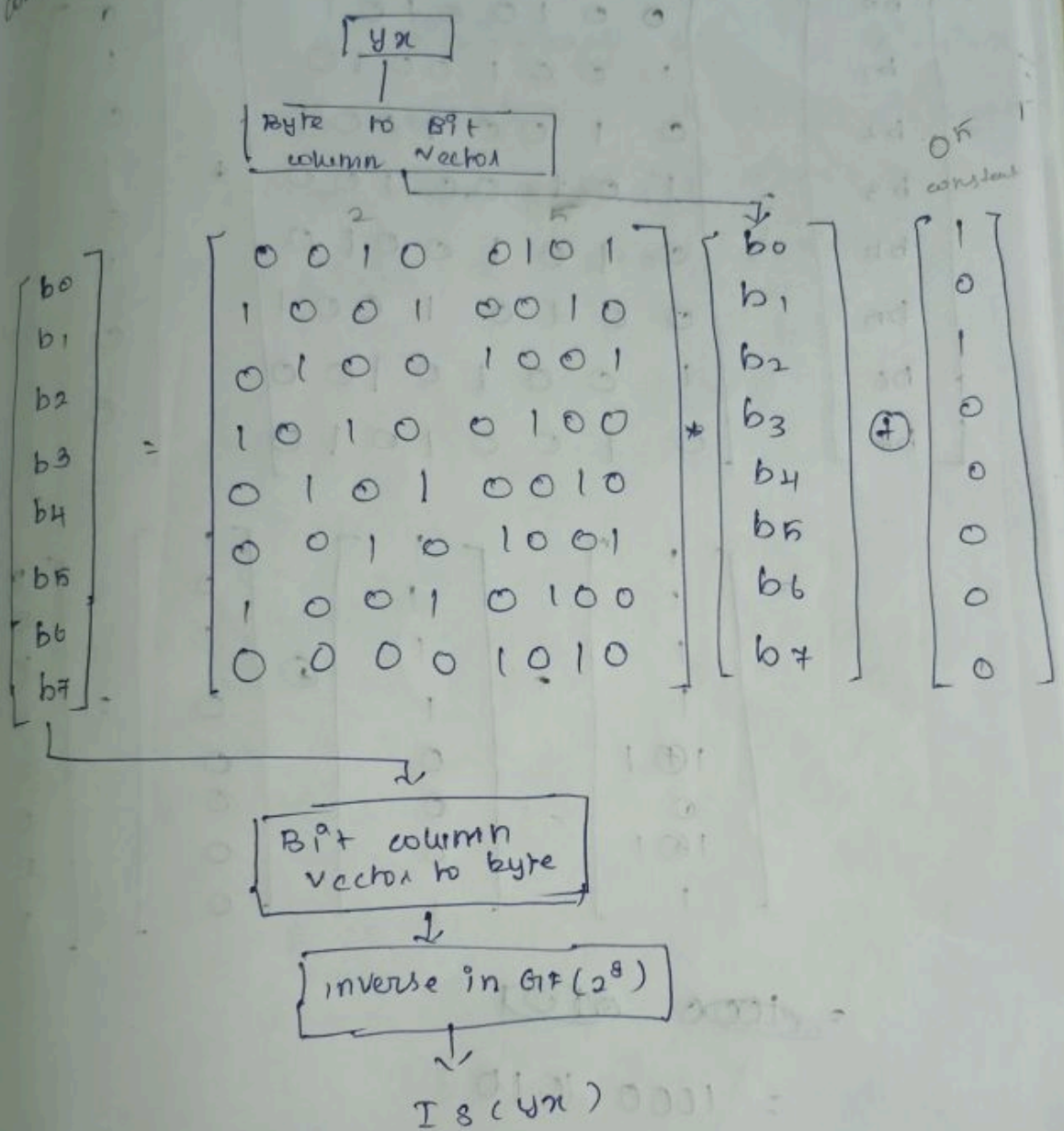
$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} =$$

example

$2A \Rightarrow$

find

Construction of IS Box



example

2A => 0010 1010

find IS(2A)

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \end{bmatrix} * \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

$$= \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \oplus 1 \\ 0 \\ 1 \oplus 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

$= 1000\ 1010$

$= 8\ A$

$(8A)^{-1} = (1000\ 1010)^{-1} = (x^7 + x^3 + x) \bmod (x^8 + x^4 + x^3 + x + 1)$

$x^4 + x^3$

$x^7 + x^3 + x \;\big|\; x^7 + x^6 + x^5 + x^4$

$x^6 + x^5 + x^4 + x^3 + x$

$x^6 + x^5 + x^4 + x^3 + x$

0

$x^8 + x^4 + x^3 + x + 1 \;\big|\; x$

$x^8 + x^4 + x^2$

$x^3 + x^2 + x + 1$

$x^3 + x^2 + x + 1 \;\big|\; x^4 + x^3 + x^2 + x + 1$

$x \;\big|\; x^3 + x^2 + x + 1$

$x^3 + x$

1

Q

x

$x^4 + x^3$

$x^2 + x + 1$

AES:

Q	A_1	A_2	A_3	B_1	B_2	B_3
—	1	0	$x^8+x^4+x^3+x+1$	0	1	x^7+x^3+x
x	0	1	x^7+x^3+x	1	x	x^8+x^2+x+1
x^4+x^3	1	x	x^3+x^2+x+1	x^4+x^3	x^5+x^4+1	x
x^2+x+1	x^4+x^3	x^5+x^4+1	$\cdot x$	x^6+x+1	$x^7+x^4+x^2+1$	1

↓ M1

$= \frac{10010101}{9 \quad 5}$

$=$

AES: types of Questions

1) SIB

2) SIR

3) MC: nomark

4) ARK

key expansion
Shor
ic bor

UNIT-3

Public key cryptosystem :

↳ Asymmetric key cryptosystem

↳ 2 - different keys

↳ public key

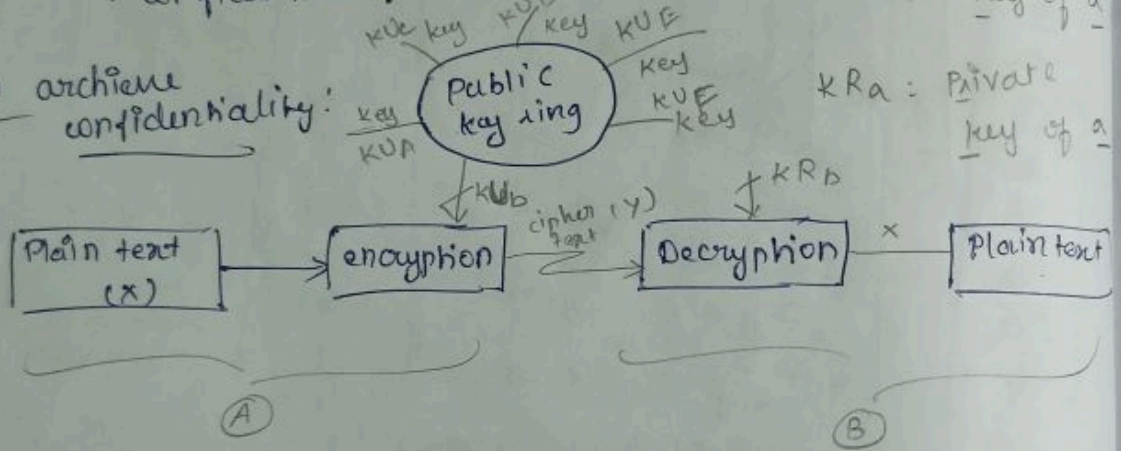
↳ private key

→ confidentiality + Authentication

KUa = Public key of a

KRa = Private key of a

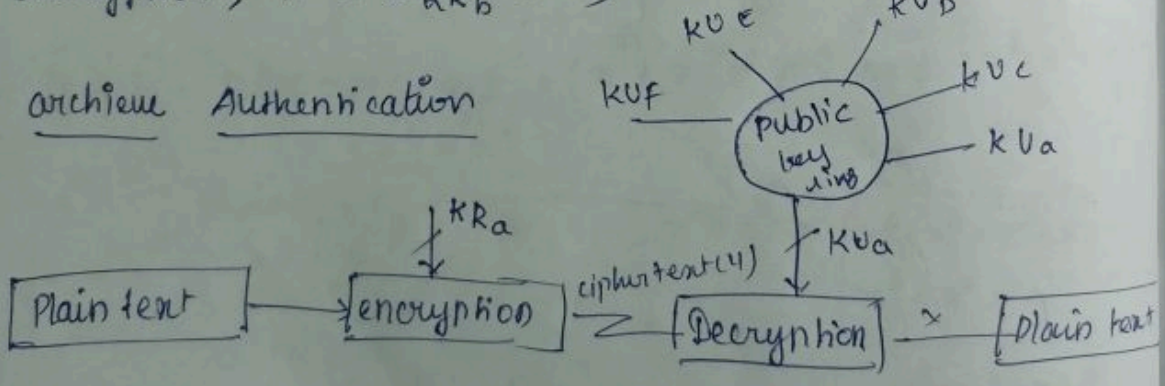
to archieve confidentiality :



encryption, $Y = E_{KU_b}(X)$

decryption, $X = D_{KR_b}(Y)$

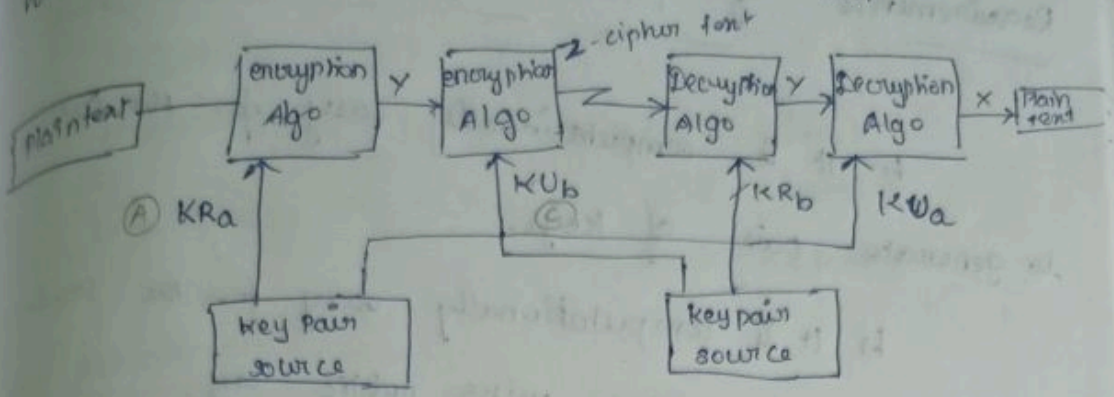
to archieve Authentication



a $Y = E_{KRa}(X)$

b $X = D_{KUa}(Y)$

to archieve confidentiality and authentication,



encryption, $Z = E_{KU_b}(E_{KR_a}(X))$

decryption, $X = D_{KU_a}(D_{KR_b}(Z))$

Symmentric key cryptosystem	Public key cryptosystem.
* same algorith with same key is used for encryption & decryption	* different algorithm is used for encryption and decryption, with pair of key
* sender & reciever must share the key value	* sender & reciever must have one of the matched pair of key.
* key must be kept secret	* one of the 2 keys must be kept secret
* knowledge of the algorithm & samples of cipher text must be insufficient to determine the key.	* knowledge of the algorithm and one of the key samples of cipher text must be insufficient to determine the key

Requirements of public key cryptosystem

- It is computationally easy for the user to generate pair of keys.
- It is computationally easy for the sender to encrypt the message using public key.
- It is computationally easy of the receiver to decrypt the cipher text using private key to recover the original message.
- It is computationally infeasible for an opponent knowing the public key to determine the ~~public~~ private key.
- It is computationally infeasible for an opponent knowing the public key and cipher text to recover the original message

Applications of public key cryptosystem:

1. Encryption / Decryption → RSA, ECC, Elgamal
2. Digital signature → DSA, schnorr, DS, Elgamal
3. Key exchange → DH key exchange
   ↓
   Diffie-hellman

RSA :

↳ pu

↳ de

↳ publ

key generat

① select

② calculat

③ calculat

④ choose

⑤ Determi

Encryptio

C

Decryptio

M

RSA :

- public key Algorithm
- developed in 1977 by Ron Rivest, Adi Shamir, Len Adleman
- published in 1978

Key generation :

1. select 2 large prime nos p, q, $p \neq q$
2. calculate $n = p \times q$
3. calculate $\phi(n) = (p-1) * (q-1)$ → euler's totient function
4. choose public key (e), $1 < e < \phi(n)$ conditions
   $GCD(\phi(n), e) = 1$
5. Determine private key (d) $e^{-1} \equiv 1 \bmod \phi(n)$

Encryption

$$C = M^e \bmod n$$

Decryption

$$M = C^d \bmod n$$

key generation.

① $p = 3$ $q = 5$

② $n = 3 \times 5$

$n = 15$

③ $\phi(15) = (3-1) * (5-1)$

$\phi(15) = 8$

$\Sigma 1, (2, 4, 7, 8), 11, 13, 14$

④ GCD $(8, 2) = (2, 0) = 2$ ✗

GCD $(8, 4) = (4, 0) = 4$ ✗

GCD $(8, 7) = (7, 1) = (1, 0) = 1$ ✓

$e = 7$

⑤ $e^{-1} \bmod \phi(n) = 1$

$7^{-1} \bmod 8 = 1$

$7 \bmod 8 = 1$

$d = 7$

Q	A	B	R	T
	8	7	1	0
7	7	1	0	1
- 1	0	-	7	8

$-1 + 8 = 7$

GCD (8, 2)

(2, 0)

$2 \overline{)8}\ 4$

8

0

GCD (8, 7)

(7, 1)

$7 \overline{)8}\ 1$

7

1

Prob

① $p = 3 \quad q = 13$

② $n = 3 \times 13$

$n = 39$

③ $\phi(39) = (3-1) * (13-1)$

$= 2 * 12$

$= 24$

{1, 2, 4, 5, 7, 8, 10, 11, 14, 16, 17, 19, 20, 22, 23, 25, 28, 29, 31, 32, 34, 35, 37, 38}

④ GCD (24, 2) = 2 ✗

GCD (24, 4) = 4 ✗

GCD (24, 5) = (5, 4) = (4, 1) = (1, 0) = 1 ✓

$e = 5$

⑤ $e^{-1} \bmod \phi(n) = 1$

$5^{-1} \bmod 39 = 1$

$d = 5$

ii) $M = 12$

$C = 12^5 \bmod 39$

$= 12^2 \bmod 39 = 144 \bmod 39$

$= 27$

$= [27 \times 27 \times 12] \bmod 39$

$= 8748 \bmod 39$

$C = 12$

In a public key system using RSA, you intercepted the cipher text $C = 8$ sent to a user whose public key is, $e = 13$ $n = 33$, what is the plain text.

Sol $e = 13$ $n = 33$ $C = 8$ $m = ?$

~~$C = m^e \bmod n$~~

$M = c^d \bmod n$

$d = 17$

$M = 8^{17} \bmod 33$

$= [\, 8^5 \bmod 33 \times 8^5 \bmod 33 \times 8^5 \bmod 33 \times 8^2 \bmod 33 \,] \bmod 33$

$= [32 \times 32 \times 32 \times 31] \bmod 33$

$M = 2$

$13^{-1} \bmod 20$

$d = 17$

Perform encryption and decryption using RSA for the following p = 7 q = 13 e = 5 M = 8

① p = 7 q = 13

② n = 7 × 13 = 91

③ $\phi(91) = 6 \times 12 = 72$

Ie 1, 2, 3, 4, 5, 6, 8, 9, 10, 11, 12, 15, 16, 17, 18, 19, 20, 22, 23, 24, 25, 27, 29, . . . 3

$C = M^e \bmod n$

$= 8^5 \bmod 91$

$= 32768$

$C = 8$

Q	A	B	R	T_1	T_2	T
14	72	5	2	0	1	-14
2	5	2	1	1	-14	29
2	2	1	0	-14	29	
		1	0		29	

$M = C^d \bmod n$

$= 8^{29} \bmod 91$

$= (8^{10} \bmod 91 \times 8^{10} \bmod 91 \times 8^9 \bmod 91) \bmod 91$

$= 8^5 \bmod 91 \times 8^5 \bmod 91 \times 8^5 \bmod 91$

$\times 8^5 \bmod 91 \times 8^5 \bmod 91 \times 8^4 \bmod 91$

$= (8 \times 8 \times 8 \times 8 \times 8 \times 1) \bmod 91$

$M = 8$

Prob

In an RSA system the public key of a given user is $e = 31$, $n = 3599$. What is the private key of this user.

Sol

$p = 59 \quad q = 61$

$\phi(n) = 58 \times 60 = 3480$

$d = e^{-1} \bmod \phi(n)$

$= 31^{-1} \bmod 3480$

$d = 3031$

Q	A	B	R	T_1	T_2	T
112	3480	31	8	0	1	-112
3	31	8	7	1	-112	337
1	8	7	1	-112	337	-449
7	7	1	0	337	-449	

$1 - (-112 \times 3)$

$-112 - (337 \times 1)$

$T_1 - T_2 \times Q$

$0 - (1 \times -112)$

$0 - 112$

Prob

encrypt the message block $M = 3$, using RSA with $p = 157 \quad q = 167, \; e = 19$

(a) $n = 157 \times 167 = 26219$

$\phi(26219) = 156 \times 166 = 25896$

$C = M^e \bmod n$

$= 3^{19} \bmod 26219$

$= (3^{10} \bmod 26219 \times 3^{9} \bmod 26219) \bmod 26219$

$= (6611 \times 19683) \bmod 26219$

$C = 25635$

Perform encryption and decryption using RSA algorithm.

$p = 7$, $q = 11$, $e = 17$, $M = 8$

$n = 77$ $\quad \phi(n) = 60$

Encryption $C = M^e \bmod n$

$= 8^{17} \bmod 77$

$= 57$

$e^{-1} \bmod \phi(n) = 1$

$17^{-1} \bmod 60 =$

$d = 53$

$P = C^d \bmod n$

$= 57^{53} \bmod 77$

$= (57^5 \bmod 77)^{10} (\quad \bmod 77)$

$= (11 * 57^3 \bmod 77) \bmod 77$

$= (11 * 8) \bmod 77$

$-3 - (4 \times 1)$
$1 - (3 \times 1)$
$0 - (1 \times 3)$
$T_1 - T_2 \times Q$

Q	A	B	R	T_1	T_2
3	60	17	9	0	1
1	17	9	8	1	-3
1	9	8	1	-3	4
8	8	1	0	4	-7

$= 1^0$

Primitive Root:

If a number's order (mod n) is $\phi(n)$, this number is called primitive root of n.

~~If $\phi(n)$ is the least positive~~

Such that $a^m \equiv 1 \bmod n$ then a is called primitive root of modulo n.

example: $n=7 \quad \phi(n)=6$

$\phi(7) = \{1, 2, 3, 4, 5, 6\}$ find primitive root

$1^1 \bmod 7 = 1$ ✗

$2^1 \bmod 7 = 2$

$2^2 \bmod 7 = 4$

$1^3 \bmod 7 = 1$ ✗

$4^1 \bmod 7 = 4$

$4^2 \bmod 7 = 2$

$4^3 \bmod 7 = 1$ ✗

$6^1 \bmod 7 = 6$

$6^2 \bmod 7 = 1$ ✓

$3^1 \bmod 7 = 3$

$3^2 \bmod 7 = 2$

$3^3 \bmod 7 = 6$

$3^4 \bmod 7 = 4$

$3^5 \bmod 7 = 5$

$3^6 \bmod 7 = 1$ ✓

$5^1 \bmod 7 = 5$

$5^2 \bmod 4 = 4$

$5^3 \bmod 7 = 6$

$5^4 \bmod 7 = 2$

$5^5 \bmod 7 = 3$

$5^6 \bmod 7 = 1$ ✓

∴ 3 & 5 are primitive root of modulo

Ans: $n = 14$

$n = 2 \times 7$

$\phi(n) = 6 = \{1, 3, 5, 9, 11, 13\}$

$1^1 \bmod 14 = 1$ ✓

$3^1 \bmod 14 = 3$

$3^2 \bmod 14 = 9$

$3^3 \bmod 14 = 8\ 13$

$3^4 \bmod 14 = 11$

$3^5 \bmod 14 = 5$

$3^6 \bmod 14 = 1$ ✓

$9^1 \bmod 14 = 9$

$9^2 \bmod 14 = 11$

$9^3 \bmod 14 = 1$ ✗

$5^1 \bmod 14 = 5$

$5^2 \bmod 14 = 11$

$5^3 \bmod 14 = 13$

$5^4 \bmod 14 = 9$

$5^5 \bmod 14 = 3$

$5^6 \bmod 14 = 1$ ✓

$11^1 \bmod 14 = 11$

$11^2 \bmod 14 = 9$

$11^3 \bmod 14 = 1$

$13^1 \bmod 14 = 13$

$13^2 \bmod 14 = 1$ ✗

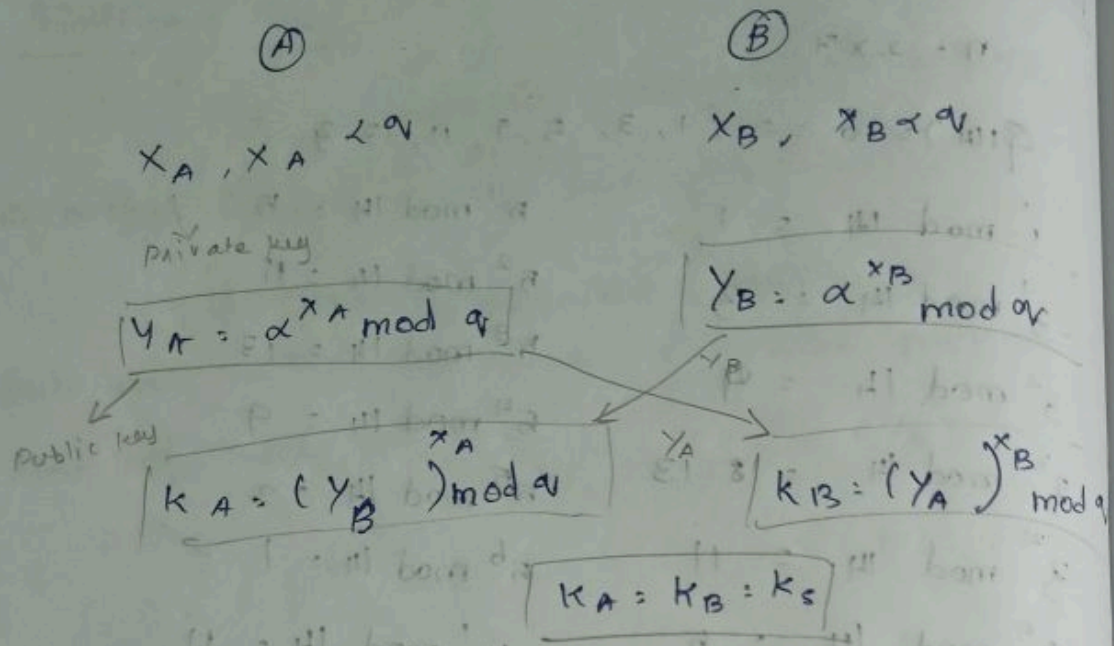
∴ 3 & 5 are primitive root.

DH key exchange:

- developed by diffie hellman
- exchanging key
- not used for EID

Publicly known values:

α → primitive root q → prime no



Users A and B use DH technique with a common prime $q = 71$ and primitive root $\alpha = 7$

(i) if user A has private key, $X_A = 5$
what is the public key of user A, (Y_A)?

(ii) if user B has private key $X_B = 12$
what is the public key of user B, $(Y_B) = ?$

(iii) what is the shared secrete key

$Y_A = \alpha^{X_A} \bmod q$
$= 7^5 \bmod 71$
$= 51$

$Y_B = \alpha^{X_B} \bmod q$
$= 7^{12} \bmod 71$
$= 4$

$K_A = 4^5 \bmod 71$

$= 30$

$K_B = 51^{12} \bmod 71$

$= (41 \times 41 \times 41 \times 41 \times 41) \bmod 71$

$= 30$

$K_A = K_B = 30$

consider a DH scheme, a common prime $q = 11$, $a = 2$.

i) show that 2 is a primitive root of 11

ii) if user A has public key $Y_A = 9$, what is A's private key

iii) if user B has public key $Y_B = 3$ what is B's private key

iv) what is the shared secrete key.

$\phi(11) = \{1, 2, 3, \ldots, \infty\}$

$2^1 \bmod 11 = 2$

$2^2 \bmod 11 = 4$

$2^3 \bmod 11 = 8$

$2^4 \bmod 11 = 5$

$2^5 \bmod 11 = 10$

$2^6 \bmod 11 = 9$

$2^7 \bmod 11 = 7$

$2^8 \bmod 4 = 3$

$2^9 \bmod 11 = 6$

$2^{10} \bmod 11 = 1$

$\therefore$ 2 is a primite root of 11.

(2)

$Y_A = \alpha^{X_A} \bmod q$

$9 = 2^{X_A} \bmod 11$

$X_A = 6$ integer (i)

$Y_B = \alpha^{X_B} \bmod q$

$3 = 2^{X_B} \bmod 11$

$X_B = 8$

(3)

$K_A = (Y_B)^{X_A} \bmod q$

$= (3)^6 \bmod 11$

$K_A = 3$

$K_B = (Y_A)^{X_B} \bmod q$

$= (9)^8 \bmod 11$

$K_B = 3$

$K_A = K_B = 3$

Man in the Middle Attack :

(1) Darth generates 2 random integers X_{D_1} & X_{D_2} & calculates $Y_{D_1} = \alpha^{X_{D_1}} \bmod q$, $Y_{D_2} = \alpha^{X_{D_2}} \bmod q$

(2) Alice $\xrightarrow{Y_A}$ Bob

(3) Darth intercepts Y_A, Darth $\xrightarrow{Y_{D_1}}$ Bob and calculates $K_2 = (Y_A)^{X_{D_2}} \bmod q$

(4) Bob receive Y_{D_1} & calculates $K_1 = (Y_{D_1})^{X_B} \bmod q$.

(5) Bob

(6) Darth and

(7) Alice

Elgamma

(A) → receiver

(1) user A

(2) calculat

(B) → sender

(1) user B

(2) compu

(3) calculat

(A)

(1) Recover

(2) calculat

example

given :

sol

(1) X_A

(2) Y_A

Y_A

Elgamal Algorithm

- when A generates a random integer X_A, $X_A < q$
- calculate $Y_A = \alpha^{X_A} \bmod q$

- when B selects a random integer k, $k < q$
- computes one-time key (k), $K = (Y_A)^k \bmod q$
- calculate $C_1 = \alpha^k \bmod q$

$C_2 = KM \bmod q$

- recovers the key, $K = C_1^{X_A} \bmod q$
- calculate $M = K^{-1} C_2 \bmod q$.

example

given: $q = 19$ $\alpha = 10$ $X_A = 5$ $k = 6$ $M = 17$

① $X_A = 5$

② $Y_A = 10^5 \bmod 19$

$Y_A = 3$

encryption

① $6 < 19$

② $K = 3^6 \bmod 19$

$K = 7$

③ $c_1 = \alpha^K \bmod q$

$= 10^6 \bmod 19$

$c_1 = 11$

$c_2 = KM \bmod q$

$= 7.17 \bmod 19$

$c_2 = 5$

(B) $\xrightarrow{11, 5}$ (A)

decryption

① $K = c_1^{X_A} \bmod q$

$= 11^5 \bmod 19.$

$K = 7$

② $M = K^{-1} c_2 \bmod q$

$= 11 \times 5 \bmod 19$

$M = 17$

$-2 = (3 \times 1)$

$1 = (-2 \times 1)$

$0 = (1 \times 1)$

$T_1 = T_2 \times Q$

Q	A	B	R	T_1	T_2	T
2	19	7	5	0	1	-2
1	7	5	2	1	-2	3
2	5	2	1	-2	3	-8
2	2	1	0	3	-8	

$= -8$

$-8 + 19 = 11$

Consider an
prime, $q = 71$
(i) If user B ha
choose the ra
cipher text

- (ii)

$q = 71$

$M = 30$

$c_1 = \alpha$

$= 7$

$c_1 = 9$

$c_2 =$

$=$

$c_2 = 2$

(ii) If user
so that e
what

Consider an elgamal scheme with common prime, $q = 71$ and primitive root $\alpha = 7$

(i) If user B has public key $Y_B = 3$ and user A choose the random integer $K = 2$. what is the cipher text of Message, $M = 30$?

Ans (i) $q = 71$ $\alpha = 7$ $K = 2$ $Y_B = 3$

$M = 30$

$C_1 = \alpha^K \bmod q$

$= 7^2 \bmod 71$

$C_1 = 49$

$k = (Y_A)^K \bmod q$

$= (3)^2 \bmod 71$

$k = 9$

$C_2 = KM \bmod q$

$= 9 \cdot 30 \bmod 71$

$C_2 = 57$

(ii) If user A now chooses a different value of K so that encoding of message $M = 30$ is $(49, \$ C_2)$ what is integer C_2?

$C_1 = \alpha^K \bmod q$

$49 = 7^K \bmod 71$

$K = 3$

$K = (Y_A)^K \bmod q$

$= (3)^3 \bmod 71$

$K = 27$

$C_2 = KM \bmod q$

$= 27 . 30 \bmod 71$

$C_2 = 29$

Make use of elgamal crypto system to perform encryption & decryption b/w angelin & Bobby. angeline generates a public private key pair, Bobby encrypts using angeline public key. angelin decrypts using her private key. using the following data the global primitive elements are $q = 7$, $\alpha = 5$, private key $X_A = 3$ random integer $K = 6$, $M = 4$.

~~$K = (Y_A)^K \bmod q$~~

~~$= (3)^6 \bmod 7$~~

~~$K = 1$~~

$Y_A = \alpha^{X_A} \bmod q$

$= 5^3 \bmod q$

$Y_A = 6$

encrypt

$k = (6)^6 \bmod 7$

$k = 1$

$c_1 = \alpha^k \bmod q$

$= 5^6 \bmod 7$

$= 1$

$c_2 = KM \bmod q$

$= 1 \times 4 \bmod 7$

$= 4 \bmod 7$

$c_2 = 4$

decrypt

$k = c_1^{xA} \bmod q$

$= 1^3 \bmod 7$

$k = 1$

$M = k^{-1} c_2 \bmod q$

$= 4 \bmod 7$

$M = 4$

Based on the following happening where Jenny generates a public and private key pair, margret encrypts using Jenny's public key and Jenny decrypt using her private key, using RSA compute encryption & decryption with following data

$P = 3 \quad q = 19 \quad M = 6, \quad e \& d = ?$

perform encryption / decryption.

Sol

① P = 3 q = 19

② n = 3 × 19

= 57

③ Φ(n) = 2 × 18

= 36

{ 1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 20, 22, 23, 25, 26, 28, 29, ... }

④ GCD (36, 2) = (2, 0) = 2

GCD (36, 4) = 4

GCD (36, 5) = 1

∴ e = 5

Q	A	B	R	T_1	T_2	T
7	36	5	1	0	1	-7
5	5	1	0	1	-7	36
-	1	0	-	7		

⑤ $e^{-1} \bmod \Phi(n) = 1$

$5^{-1} \bmod 36$

d = 29

encryption : $C = M^e \bmod n$

$= 6^5 \bmod 57$

= 41

decryption:

$M = c^d \bmod n$

$= 24^{29} \bmod 57$

$= (9 \times 9 \times 9 \times 9 \times 9 \times 36) \bmod 57$

$= 2125764 \bmod 57$

$= 6$

$24^{29} \bmod 57 = 7962624$

$24^{29} \bmod 57 = 9$

perform a successfull DH key exchange b/w andrew and bobby as per the following scenario lets consider that both have mutually selected the numbers as q & α which are 11 & 3 respectively. assume andrew has a secrete key and bobby has a secret key which are 4 & 8 repectively. apply the steps key exchange b/w them.

sol

gn: $q = 11$, $\alpha = 3$ $\quad X_A = 4 \quad X_B = 8$

$Y_A = 3^4 \bmod 11$

$= 4$

$K_A = (4)^4 \bmod 11$

$= 9$

$Y_B = \alpha^{X_B} \bmod q$

$= 3^8 \bmod 11$

$= 5$

$K_B = (4)^8 \bmod 11$

$= 9$

$K_A = K_B = 9$

determine $w_{16}, w_{17}, w_{18}, w_{19}$ (round 4) in AES encryption

w_{12}	w_{13}	w_{14}	w_{15}
C0	89	57	B1
AF	2F	51	AE
DF	63	AD	7E
39	67	06	C0

S-box output of w_{15} - E4 F3 BA C8

$g[w[15]] \Rightarrow$ { B1 AE 7E C0 }

Circular left shift ① => { AE 7E C0 B1 }

S-box ② => { E4 F3 BA C8 }

③ => { 08 00 00 00 }

$g[w[15]]$ = EC F3 BA C8

1110 0100
0000 1000
1110 1100
E C

$w[16] = w[12] \oplus g[w[15]]$

$w[12]$ = 1100 0000 (C0) 1010 1111 (AF) 1101 1111 (DF) 0011 1001 (39)

$g[w[15]]$ = 1110 1100 (EC) 1111 0011 (F3) 1011 1010 (BA) 1100 1000 (C8)

0010 1100 (2C) 0101 1100 (5C) 0110 0101 (65) 1111 0001 (F1)

~~0010 11~~

$w[16]$ 2C 5C 65 F1

prob

perform

decryptio

A3 =>

$w[17] =$

$w[13] =$

$w[16] =$

$w[17] =$

$w[18] =$

$w[14] =$

$w[17] =$

$w[18]$

$w[19] =$

$w[15] =$

$w[18]$

w[17] = w[16] + w[13]

	1000 1001	0010 1111	0110 1011	0110 0111
w[13] =	89	2F	6B	67
w[16] =	0010 1100	0101 1100	0110 0101	1111 0001
	2C	5C	65	F1
	1010 0101	0111 0011	0000 1110	1001 0110
w[17] =	A5	73	0E	96

w[18] = w[14] + w[w17]

	0101 0111	0101 0001	1010 1101	0000 0110
w[14] =	57	51	AD	06
w[17] =	A5	73	0E	96
	1111 0010	0010 0010	1010 0011	1001 0000
w[18]	F2	22	A3	90

w[19] = w[15] + w[18]

	1011 0001	1010 1110	0111 1110	1100 0000
w[15] =	B1	AE	7E	C0
w[18] =	F2	22	A3	90
	0100 0011	1000 1100	1101 1101	0101 0000
	43	8C	DD	50

Perform inverse s-box calculation in AES decryption for the value A3

A3 => (1010 0011)

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \end{bmatrix} * \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \oplus 1 \\ 1 \\ 1 \oplus 1 \\ 1 \oplus 1 \\ 1 \\ 1 \\ 1 \oplus 1 \\ 1 \end{bmatrix}$$

$$\begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \end{bmatrix} = 10111011$$

$$(B7)^{-1} = (10110111)^{-1} = (x^7 + x^5 + x^4 + x^2 + x + 1) \bmod (x^8 + x^4 + x^3 + x + 1)$$

	A	B	R	T_1	T_2	T
Q	$x^8+x^4+x^3+x+1$	$x^7+x^5+x^4+x^2+x+1$		0	1	$-x$
x		$x^6+x^5+x^4+x^2+1$				
	$x^7+x^5+x^4+x^2+x+1$	$x^6+x^5+x^4+x^2+1$		1	$-x$	x^2+1
2		$x^6+x^4+x^3+x^2+1$				
	$x^6+x^5+x^4+x^2+1$	x^5+x^3		$-x$	x^2+1	$-x^2-x-1$
1						
	$x^6+x^4+x^3+x^2+1$	x^5+x^3		x^2+1	$-x^2-x-1$	x^3+x+1
2		x^3+x^2+1				
2+x	x^5+x^3	x^3+x^2+1	x^2+x	$-x^2-x-1$	x^3+x+1	$-(x^5+x^4+x^3+x^2+1)$
	x^3+x^2+1	x^2+x	1	x^3+x+1 $-(x^5+x^4+x^3+x^2+1)$	$-(x^5+x^4+x^3+x^2+1)$	$x^6+x^5+x^4+1$
x	x^2+x	1	0	$-(x^5+x^4+x^3+x^2+1)$	$(x^6+x^5+x^4+1)$	
x+1		0	—	$(x^6+x^5+x^4+1)$		
	1			↓ MI		

$= 0111\ 0001$

$= 71$