"27"

Lecture

Not always multiplication

Symbolic only

* Algebraic structure $\langle G, * \rangle$ is called a group if it satisfies following properties

1. Closure

If $\forall a, b \in G$, $a * b \in G$

$\Rightarrow *$ is closed with respect to G.

2. Associativity

If $\forall a, b, c \in G$

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

then $*$ satisfies associativity

3. Identity

$\forall a \in G$ $\exists e \in G$ such that

$$a * e = a = e * a$$

4. Inverse

$\forall a \in G$, $\exists b \in G$ such that

$$a * b = b * a = e$$

E.g. $\langle Z, + \rangle$

Set of Integers $Z = \{\ldots, -3, -2, -1, 0, 1, 2, \ldots\}$

Is $\langle Z, + \rangle$ Group?

→ Yes because

(1) If you add any two elements in Z, the answer is also in Z.

(2) $+$ is associative i.e.

$\forall a, b, c \in Z$

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

(3) $0 \in Z$ is Identity of '$+$'

$\forall a \in Z$, $0 \in Z$ is such that

$a+0 = 0+a = a$

(4) $\forall a \in Z, \exists b \in Z$ such that

$a+b = 0$

i.e. $\boxed{b = -a}$ exist in Z

$\therefore \langle Z, + \rangle$ is group.

E.g. $\langle N, + \rangle$

$N = \{1, 2, 3, \ldots\}$ is not a group

E.g. $\langle Z, * \rangle$

Multiplication

It is not group because

$2 \in Z$ but inverse $\frac{1}{2} \notin Z$

E.g. $\langle R, * \rangle$

Set of Real Numbers

(i) R

$\forall a, b \in R, \; a * b \in R$

(ii) Mult. is associative

$\forall a, b, c \in R, \; (a * b) * c = a * (b * c)$

(iii) Identity $= 1$

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

(iv) Inverse of any element must exist in R.

$0^{-1} = \frac{1}{0}$ is Not defined

$\therefore \langle R, * \rangle$ is not group

E.g. $\langle R, + \rangle$ is group E.g. $\langle Z, + \rangle$ is also group.

If In addition to 4 properties, algebraic structure satisfies Commutative property then the group is known as Abelian Group

★ 5th property: If $\forall a, b \in G$

$a * b = b * a$ then

$*$ is Commutative.

Eg. $\langle Z, + \rangle$ is Abelian group

$\langle R, + \rangle$ is Abelian group

Group

Infinite

Eg. $\langle Z, + \rangle$

$\langle R, + \rangle$

Number of elements in Z, R are Infinite.

Finite

Eg. $\langle Z_5, +_5 \rangle$

$\langle Z_5^*, *_5 \rangle$

→ Very Important for Cryptography

① $\langle Z_5, +_5 \rangle$ → Addition Modulo 5

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

(I) $\forall a, b \in Z_5 \quad a +_5 b$ i.e. $(a+b) \% 5 \in Z_5$

$\Rightarrow$ closure satisfied

(II) $\forall a, b, c \in Z_5$

$(a +_5 b) +_5 c = a +_5 (b +_5 c)$

(III) $\forall a \in Z_5$, $0 \in Z_5$ is such that

$a +_5 0 = a = 0 +_5 a$

(IV) $\forall a \in Z_5$, $\exists b \in Z_5$ such that

$a +_5 b = 0$ e.g. $a=2, b=3$
$a=1, b=4$

$+_5$	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

From this Table we can conclude that $\langle Z_5, +_5 \rangle$ is Group

E.g. $Z_5^* = \{1,2,3,4\}$ Operator $*_5$

Multiplication Modulo 5

$*_5$	1	2	3	4
1	1	2	3	4
2	2	4	6%5 = 1	3
3	3	1	4	2
4	4	3	2	1

(I) We can see $(a*b) \bmod 5 \in Z_5^*$
$\Rightarrow$ closure satisfied

(II) $(a *_5 b) *_5 c = a *_5 (b *_5 c)$
$\forall a, b, c \in Z_5^*$

(III) 1 is Identity of $*$
$1 \in Z_5^*$

(IV) $\bar{1}^{-1} = 1 \quad \bar{2}^{-1} = 3 \quad \bar{3}^{-1} = 2 \quad \bar{4}^{-1} = 4$
$\therefore$ Inverse exist

$\therefore \langle Z_5^*, *_5 \rangle$ is group.

→ Generally we don't write $*_5$ but just write $*$.

→ In addition $*$ is Commutative

∴ $\langle Z_5^*, *_5 \rangle$ is Group and Abelian Group.

★ $\langle Z_n^*, * \rangle$ where n is prime and $*$ is Multiplication modulo n is Abelian Group.

E.g. $Z_7^* = \{1, 2, 3, 4, 5, 6\}$

$*_7$	1	2	3	4	5	6
1	(1)	2	3	4	5	6
2	2	4	6	(1)	3	5
3	3	6	2	5	(1)	4
4	4	(1)	5	2	6	3
5	5	3	(1)	6	4	2
6	6	5	4	3	2	(1)
$1^{-1}=1$	$2^{-1}=4$	$3^{-1}=5$	$4^{-1}=2$	$5^{-1}=3$	$6^{-1}=6$	

We can see from this that It is group.

$\langle Z_5, +_5 \rangle$
$\langle Z_5^*, *_5 \rangle$
} are finite groups

✱ Order of a group G

It is the number of elements in the Group.

Order of $\langle Z_5, +_5 \rangle$ is 5

Order of $\langle Z_5^*, *_5 \rangle$ is 4

✱ Subgroup of Group G

A subset H of a group G is a Subgroup of G if H is itself a group with respect to the Operation on G.

Group $G = \langle S, \circ \rangle$
Sub Group $H = \langle T, \circ \rangle$
} In other words

$T \neq$ Empty set.
$\circ$ is same

Q. Is $H = \langle Z_{10}, + \rangle$ a subgroup $\langle Z_{12}, + \rangle$?

→ No because + in Z_{10} is $+_{10}$ while + in Z_{12} is add. Mod 12 i.e. $+_{12}$

★ Cyclic Subgroups :- If a subgroup of a group can be generated using the power of an element, the subgroup is called the cyclic subgroup.

→ Power Here means repeatedly applying the group operation to the element

E.g. $a^n = a \circ a \circ a \cdots \circ a$ (n times)

$a^5 = a+a+a+a+a$ (If $\circ = +$)

$a^5 = a*a*a*a*a$ (If $\circ = *$)

$a^0 = e$ (Identity)

→ Important for Asymmetric Cryptography

Ex 1 $G = \langle Z_6, + \rangle$, $Z_6 = \{0,1,2,3,4,5\}$

→ Cyclic Subgroup generated by 0

$0^0 \text{ MOD } 6 = 0$

$0^1 \text{ MOD } 6 = 0$

∴ Subgroup is $\langle \{0\}, + \rangle$

Note: + operator is used

→ Cyclic Subgroup generated by 1

1^0 MOD 6 = 0 (∵ 0 is Identity of +)

1^1 MOD 6 = 1

1^2 MOD 6 = (1+1) MOD 6 = 2

1^3 MOD 6 = (1+1+1) MOD 6 = 3

1^4 MOD 6 = (1+1+1+1) MOD 6 = 4

1^5 MOD 6 = (1+1+1+1+1) MOD 6 = 5

Repeats
- 1^6 MOD 6 = (1+1+1+1+1+1) MOD 6 = 0
- 1^7 MOD 6 = 1
- 1^8 MOD 6 = 2
- 1^9 MOD 6 = 3
- 1^{10} MOD 6 = 4
- 1^{11} MOD 6 = 5

∴ Subgroup generated is $\langle \{0,1,2,3,4,5\}, + \rangle$

i.e. $\langle Z_6, + \rangle$

→ Cyclic Subgroup generated by 2

2^0 MOD 6 = 0

2^1 MOD 6 = 2

2^2 MOD 6 = 4

2^3 MOD 6 = 0

2^4 MOD 6 = 2

2^5 MOD 6 = 4

∴ Subgroup generated = $\langle \{0,2,4\}, + \rangle$

Note: + operator is used

→ Cyclic Subgroup generated by 3

$3^0 = 0$

$3^1 = 3$

$3^2 = (3+3) \% 6 = 0$

$3^3 = 9 \% 6 = 3$

∴ Generated Subgroup $\langle \{0,3\}, + \rangle$

→ Cyclic Subgroup generated by 4

$4^0 = 0$

$4^1 = 4$

$4^2 = (4+4) \% 6 = 2$

$4^3 = (4+4+4) \% 6 = 0$

$4^4 \% 6 = 4$

$4^5 \% 6 = 2$

∴ Generated Subgroup $\langle \{0,2,4\}, + \rangle$

→ Cyclic Subgroup generated by 5

$5^0 = 0$

$5^1 = 5$

$5^2 = 4$

$5^3 = 3$

$5^4 = 2$

$5^5 = 1$

∴ Generated Subgroup $\langle \{0,1,2,3,4,5\}, + \rangle$

Note: x/* is Multiplication Operator

Here

Ex 2 $G = \langle Z_{10}^*, \times \rangle$. check for group

$Z_{10}^* = \{1, 3, 7, 9\}$

MOD 10	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

→ Table shows that all properties are satisfied ⇒ It is Group.

→ Cyclic Subgroup generated by 1

1^0 MOD 10 = 1 (e=1)

1_1^1 MOD 10 = 1

1^2 MOD 10 = (1 * 1) = 1

∴ Subgroup = $\langle \{1\}, \times \rangle$ Generated by 1

→ Subgroup generated by 3 :-

$3^0 = 1$

$3^1 = 3$

$3^2 = (3*3) \text{ MOD } 10 = 9$

$3^3 = (3*3*3) \text{ MOD } 10 = 7$

will repeat

$3^4 = (3*3*3*3) \text{ MOD } 10 = 1$

$3^5 = 243 \text{ MOD } 10 = 3$

∴ Subgroup generated by 3 $= \langle \{1, 3, 7, 9\}, \times \rangle$

→ Subgroup generated by 7 :-

$7^0 = 1$

$7^1 = 7$

$7^2 = 49 \text{ MOD } 10 = 9$

$7^3 = 343 \text{ MOD } 10 = 3$

$7^4 \text{ MOD } 10 = 1$

$7^5 \text{ MOD } 10 = 7$

$7^6 \% 10 = 9$

$7^7 \% 10 = 3$

∴ Subgroup generated by 7 $= \langle \{1, 3, 7, 9\}, \times \rangle$

→ Subgroup generated by g:

$g^0 \text{ MOD } 10 = 1$ }
$g^1 \text{ MOD } 10 = g$ }
$g^2 \text{ MOD } 10 = 1$ } Will Repeat
$g^3 \text{ MOD } 10 = g$ }

∴ Subgroup generated by g
$= \langle \{1, g\}, \times \rangle$

Here
Ord (1) = 1 i.e. order of 1
Ord (3) = 4
ord (4) = 4
ord (9) = 2

→ Order of element 'a' is Ord(a) is the number of elements in the subgroup generated by element a.

MOD 10

	$i=1$	$i=2$	$i=3$	$i=4$
$a=1$	(1)	1	1	1
$a=3$	3	9	7	(1)
$a=7$	7	9	3	(1)
$a=9$	9	(1)	9	1

→ $\text{ord}(1) = 1$ (∵ At $i=1$ we get 1)
$\text{ord}(3) = 4$ (∵ At $i=4$ we get 1 first time)
$\text{ord}(7) = 4$
$\text{ord}(9) = 2$ (∵ At $i=2$, we get 1 first time)

→ Table is Computed using
$a^i \bmod n$ i.e. $a^i \bmod 10$

$a \in Z_{10}^*$

$\phi(10) = 4$ (∵ $\phi(2\times5) = \phi(2)\times\phi(5)$
$= 1 \times 4$
$= 4$)

↳ ∵ There are 4 values of i.

→ Here $a=3$, $a=7$ are known as primitive roots or Generator of group $\langle Z_{10}^*, \times \rangle$

→ When order of an element is $\phi(n)$, that element is called the primitive root

→ $\phi(10) = 4$

$G = \langle Z_{10}^*, \times \rangle$

→ $\text{Ord}(3) = 4 = \phi(10)$

→ $\text{ord}(7) = 4 = \phi(10)$

∴ 3, 7 are Primitive roots or Generator

→ Primitive roots are very important for "Elgamal Cryptosystem"

Ex 2 Find the primitive roots for $\langle Z_7^*, \times \rangle$

$Z_7^* = \{1, 2, 3, 4, 5, 6\}$

$\phi(7) = 6$

MOD 7

	i=1	i=2	i=3	i=4	i=5	i=6
a=1	[1]	1	1	1	1	1
a=2	2	4	[1]	2	4	1
a=3	3	2	6	4	5	[1]
a=4	4	2	[1]	4	2	1
a=5	5	4	6	2	3	[1]
a=6	6	[1]	6	1	6	1

Ord(1)=1

Ord(2)=3

Ord(3)=6

Ord(4)=3

Ord(5)=6

Ord(6)=2

Since Ord(3)=6, Ord(5)=6 = $\phi(7)$,

3 and 5 are Primitive roots/

Generator for the Group $\langle \mathbb{Z}_7^*, \times \rangle$

☆ a=3,5 is the answer.

Result: Number of primitive roots are $\phi(\phi(n))$ for group $\langle Z_n^*, \times \rangle$ (Provided If there are any roots)

E.g. $\langle Z_{10}^*, \times \rangle$ has two roots 3, 7.

$\phi(\phi(10))$

$= \phi(4)$

$= \phi(2^2)$

$= 2^2 - 2^1$

$= \boxed{2}$ → 2 roots

E.g. $\langle Z_7^*, \times \rangle$ has two roots 3, 5

# of roots $= \phi(\phi(7))$

$= \phi(6)$

$= \phi(2 \times 3)$

$= \phi(2) \times \phi(3)$

$= (2-1) \times (3-1)$

$= \boxed{2}$

Result: The group $\langle Z_n^*, \times \rangle$ has primitive roots if n is $2, 4, p^t$ or $2p^t$ (p is prime)

Check for $n = 17, 20, 38, 50$

① $n = 17 = 17^1 = p^t \Rightarrow \langle Z_{17}^*, \times \rangle$ is group with primitive roots

② $n = 20 = 2^2 \times 5$

neither $2, 4, p^t, 2p^t$

$\therefore \langle Z_{20}^*, \times \rangle$ has no Primitive roots

③ $n = 38$

$= 2 \times 19^1$

$= 2p^t$ where $p = 19$ (Prime)

$\therefore \langle Z_{38}^*, \times \rangle$ has Primitive roots

④ $n = 50$

$= 2 \times 25$

$= 2 \times 5^2$

$= 2p^t$ where $p = 5$ (Prime)

$\therefore \langle Z_{50}^*, \times \rangle$ has Primitive Roots.

Elgamal CryptoSystem :-

→ Named after its Inventer, Taher Elgamal
→ It is based on the Discrete Logarithm problem.

☆ Key Generation :-

(1) Select p (Very large Prime)
(2) Select e_1 (Primitive root) of the group $\langle Z_p^*, \times \rangle$
(3) Select d to be a member of the group $G = \langle Z_p^*, \times \rangle$ such that $1 \leq d \leq p-2$
(4) $e_2 = e_1^d \bmod p$
(5) Public key : (e_1, e_2, p)
(6) Private key : d

Return Public and Private key

Plain Text
Number

DATE
PAGE NO

★Elgamal_Encryption (M, e_1, e_2, p)

e_1, e_2, p → Public Key

{

$C_1 = e_1^{r} \bmod p$ where r is random integer from Group $\langle Z_p^*, \times \rangle$

$C_2 = (e_2^{r} * M) \bmod p$

}

Cipher Text: C_1, C_2 (for M)

★Elgamal_Decryption (C_1, C_2, d, p)

C_1, C_2 → CipherText

{

$M = [C_2 \times (C_1^{d})^{-1}] \text{ MOD } p$

}

Correctness

$$[C_2 \times (C_1^d)^{-1}] \text{ MOD } P$$

$$= [e_2^r * M * (e_1^{rd})^{-1}] \text{ MOD } P$$

$$= [(e_1^d)^r * M * (e_1^{rd})^{-1}] \text{ MOD } P$$

$$= [e_1^{rd} * M * (e_1^{rd})^{-1}] \text{ MOD } P$$

$$= M * e_1^{rd} * (e_1^{rd})^{-1} \text{ MOD } P$$

$$= M$$

(1) Alice sends C_1, C_2 for plaintext M to Bob

(2) If Eve gets C_1, C_2 i.e.

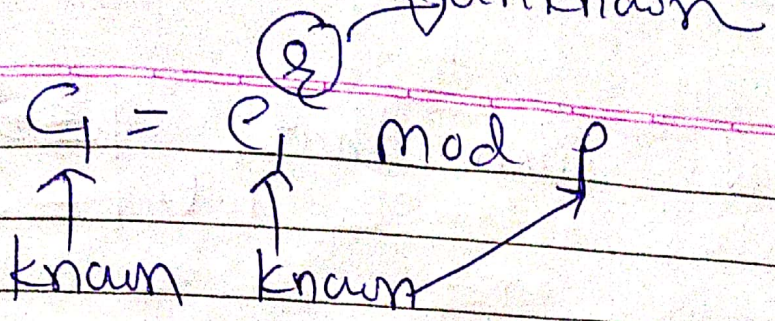
$$C_1 = e_1^r \text{ Mod } P$$

$$C_2 = (e_2^r * M) \text{ Mod } P$$

then still it is difficult to guess r.

So, Eve knows C_1, e_1, e_2, P

Public key.



To get x from c_1, e_1, p (for the above equation) is known as Discrete Logarithm problem.

DLP is Difficult to solve (NP-Hard)

E.g. Bob chooses $p = 11$.
He then chooses e_1 (Primitive Root)
i.e. $e_1 = 2$

$2^0 = 1$	$i=6$ $2^6 = 64 \% 11 = 9$
$i=1$ $2^1 = 2$	$i=7$ $2^7 = 128 \% 11 = 7$
$i=2$ $2^2 = 4$	$i=8$ $2^8 = 256 \% 11 = 3$
$i=3$ $2^3 = 8$	$i=9$ $2^9 = 512 \% 11 = 6$
$i=4$ $2^4 = 16 \% 11 = 5$	$i=10$ $2^{10} = 1024 \% 11 = 1$ (will Repeat)
$i=5$ $2^5 = 32 \% 11 = 10$	$2^{11} = 2048 \% 11 = 2$

At $i = 10$, $2^{10} \% 11 = 1$ = Identity of Multiplication.

$\therefore Ord(2) = 10 = p-1 = 11-1$

$\therefore$ 2 is the generator for $\langle Z_{11}^*, \times \rangle$

→ Select d such that, $1 \le d \le P-2$
i.e. $1 \le d \le g$

→ Let's choose $d = 3$

→

$e_1 = 2$

$e_2 = e_1^d \bmod p = 2^3 \bmod 11 = 8$

$p = 11$

∴ Public key $(e_1, e_2, P) = (2, 8, 11)$

Private key : $d = 3$

☆ Encrypt Message $M = 7$

① r is chosen from $\langle Z_{11}^*, \times \rangle$

say $r = 4$

② $C_1 = e_1^r \bmod p$

$= 2^4 \bmod 11$

$= 5$

$C_2 = (e_2^r * M) \bmod p$

$= (8^4 * 7) \bmod 11$

$= (8 \times 8 \times 8 \times 8 \times 7) \bmod 11$

$= ((8 \times 8) \bmod 11 \times 8 \bmod 11 \times (8 \times 7) \bmod 11) \bmod 11$

$= (9 \times 8 \times 1) \bmod 11$

$= 72 \bmod 11$

$= 6$

∴ Cipher text : $C_1 = 5$

$C_2 = 6$

✡ Decryption

(3) $C_1 = 5, C_2 = 6, d = 3$

Compute $[C_2 \times (C_1^d)^{-1}] \bmod p$

$= [6 \times (5^3)^{-1}] \bmod p$

$= (6 \bmod p \times 125^{-1} \bmod p) \bmod p$

$= (6 \bmod 11 \times 125^{-1} \bmod 11) \bmod 11$

$= (6 \times 4^{-1} \bmod 11) \bmod 11$

$= (6 \times 3) \bmod 11 = \boxed{7}$ which is M

☆ Attacks on Elgamal

DATE
PAGE No

(1) Low Modulus Attack

Way 1 ⇒ If p is not large enough, Eve can use Bruteforce/other algorithms to find d or r.

$$C_1 = e_1^r \bmod p$$

→ If C_1 is Intercepted by Eve and p is small, r can be guessed easily (Note: (e_1, e_2, p) is Public)

→ Now C_2 and e_2^r is available

$$\therefore C_2 = (e_2^r * M) \bmod p$$

C_2: Intercepted; $(e_2^r * M)$: Available; p: Available

$$\therefore (e_2^r)^{-1} \times C_2 \equiv M \bmod p$$

∴ M can be obtained using this.

Part 2

From key generation, we know that

$$e_2 = e_1^d \bmod p$$

Note: (e_2, e_1, p) is public

∴ If p is not large then 'd' can be obtained using Brute force or other methods for Discrete Log Problem.

(2) Known PlainText Attack:

If Alice uses same random exponent r to encrypt two plaintexts M_1, M_2 then Eve discovers M_2 if she knows M_1 + ~~C_2, C_4~~

Assume for M_1, Ciphertexts: C_1, C_2
for M_2, Ciphertexts: C_3, C_4

$$C_2 = (M_1 \times e_2^r) \bmod p.$$
$$C_4 = (M_2 \times e_2^r) \bmod p.$$

} same 'r' is used

Eve finds M_2 using following steps:

① $e_2^{2r} = (C_2 \times M_1^{-1}) \text{ MOD } P$

② $M_2 = C_4 \times (e_2^{2r})^{-1} \text{ MOD } P$

∴ It is recommended that Alice use a fresh value of r to thwart the known-plaintext attacks.

Application:

→ Encryption / Decryption of small messages

→ Key Exchange

→ Authentication

Recommended for Elgamal:

↳ Prime must be at least 300 digits

↳ r must be new for each encryption.