"Basics of Crptography"

Shubham Kumar*

October 2020

1 Set Theory:-

- Universal Set or Universe of discourse: Collection of Objects.
- Set: Collection of well-defined objects. Here the term well defined refers, the definition of a set is not person dependent.
- It can be defined using Characteristic function. This tells us that the entire (any) Mathematical structure is built on the binary logic.
- Cartesian product of two sets A and B is nothing but the set of all possible combinations of elements of A and B
- Function: Every element of domain is associated with some other (unique) element of the co-domain
- Binary Operator: $*$ is said to be a binary operator and is defined as $* : G \times G \to G$
- Arithmetic Operation: Addition, Subtraction, Multiplication, Division (all are binary operators on $\Re$)

2 Group Theory:-

Definition 2.1 *A set G with a Binary operation $*$ defined on G is said to be a **Group**, if it satisfies the following four axioms,*

- *Closure:*
$$\forall a, b \in G \Rightarrow a * b \in G$$
- *Associative:*
$$a * (b * c) = (a * b) * c, \forall a, b, c \in G$$

*Mtech-1st yr: Information Security, Atal Bihari Vajpayee Indian Institute of Information Technology and Management, Gwalior, India-474015

- *Identity: For every $a \in G$, there exists a unique element e such that, $a * e = e * a = a$, then 'e' is called as identity element*
- *Inverse: For every non-zero element a of G, there exists a unique non-zero $a' \in G$ such that,*
$$a * a' = a' * a = e$$
- *Commutative:*
$$a * b = b * a, \forall a, b \in G$$

  If a Group satisfies the Commutative property, then it is called as an Abelian Group.

2.1 Classification of a Algebraic Structure

- *Groupoid: Closure*
- *SemiGroup: Closure + Associative*
- *Monoid: Closure + Associative + Identity*
- *Group: Closure + Associative + Identity + Inverse*
- *Abelian Group: If a Group satisfies the Commutative property.*

2.2 Properties of Group

- *If a group has a finite number of elements, it is referred to as a finite group, and the order of the group is equal to the number of elements in the group. Otherwise, the group is an infinite group.*
- *Identity Element(e) is unique for a Group.*
- *Left Identity Should be same as Right Identity :*
$$a * e = e * a$$
- *a^{-1} is unique for a given element a.*
- $(a * b)^{-1} = b^{-1} * a^{-1}$
- *If G is Abelian Group than:*
$$(a * b)^{-1} = b^{-1} * a^{-1}$$
$$(a * b)^{-1} = a^{-1} * b^{-1}$$

2.2.1 Cyclic Group

- *A group G is cyclic if every element of G is a power a^k (k is an integer) of a fixed element $a \in G$. The element a is said to generate the group G, or to be a generator of G. We denote the cyclic group of order n by Z_n.*
- *A cyclic group is always an abelian group, and may be finite or infinite but and abelian group need not be cyclic group.*
- *A non-abelian group will always be non-cyclic.*

Example 2.1 *Check the following (Whether Cyclic or not)*
For $n \geq 1$ $(Z_n, \oplus)$ is cyclic
Solution: Z_n is an abelian group
For $\oplus$, Z_n generates number a_i where $a_i < n$
Then we can find a subgroup of Z_n which generates a repetative group. So, we can say that Z_n is cyclic group.

Example 2.2 *Check the following (whether Group or not)*

1. *The set of integers with usual addition*
   Solution:- Let $a, b, c \in Z$, then
   Closure Property:
   $$a + b \in Z$$
   Associative Property:
   $$a + (b + c) = (a + b) + c, \forall a, b, c \in Z$$
   Identity Property:
   $$a + 0 = 0 + a = a, \forall a \in Z$$
   Inverse Property:
   $$a + \ (-a\ ) = \ (-a\ ) + a = 0, \forall a \in Z$$
   Commutative Property:
   $$a + b = b + a, \forall a, b \in Z$$
   So, the set of integers with usual addition is not only group but it's an abelian group.

2. *The set of integers with usual multiplication*
Solution:- Let $a, b, c \in Z$, *then*
Closure Property:

$$a * b \in Z$$

Associative Property:

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

Identity Property:

$$a * 1 = 1 * a = a, \forall a \in Z$$

Inverse Property:

$$a * a^{-1} = a^{-1} * a = 1, \forall a \in Z$$

It doesn't holds because except for 1, inverse of every number is not integer it's in fraction.
Therefore, the set of integers under multiplication is not a group.

3. *The set of real numbers with usual addition*
Solution:- Let $a, b, c \in R$, *then*
Closure Property:

$$a + b \in R$$

Associative Property:

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

Identity Property:

$$a + 0 = 0 + a = a, \forall a \in R$$

Inverse Property:

$$a + \ (-a\ ) = \ (-a\ ) + a = 0, \forall a \in R$$

Commutative Property:

$$a + b = b + a, \forall a, b \in R$$

So, the set of real numbers with usual addition is not only group but it's an abelian group.

4. *The set of real numbers with usual multiplication*
Solution:- Let $a, b, c \in R$, then
Closure Property:

$$a * b \in R$$

Associative Property:

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

Identity Property:

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

Inverse Property:

$$a * a^{-1} = a^{-1} * a = 1, \forall a \in R$$

Commutative Property:

$$a + b = b + a, \forall a, b \in R$$

Therefore, the set of real numbers under multiplication is not only group but it's an abelian group.

5. *The set of natural numbers with usual addition*
Solution:- Let $a, b, c \in N$, then
Closure Property:

$$a + b \in N$$

Associative Property:

$$a + (b + c) = (a + b) + c, \forall a, b, c \in N$$

Identity Property:

$$a + 0 = 0 + a = a, \forall a \in N$$

Inverse Property:

$$a + \ (-a\ ) = \ (-a\ ) + a = 0, \forall a \in R, but except for a = 0, -a \notin N$$

So, The set of natural numbers under addition is not a group beause it does not have the inverse property .

6. $A = \{0, 1, 2, 3\}, a * b = a + b - ab$
Closure Property: For a=3 and b=3

$$a * b = a + b - ab = 3 + 3 - (3 * 3)$$

$$a * b = 6 - 9 = -3 \text{ and } -3 \notin A$$

So,it is not a group.

3 Rings:-

Definition 3.1 *A set R with two Binary operations $*_1$ and $*_2$ (denoted by $(R, *_1, *_2)$) is said to be a* **Ring***, if It satisfies the following axioms,*

- $(R, *_1)$ *is an abelian group*
- *Closure:*
$$\forall a, b \in R \Rightarrow a *_2 b \in R$$
- *Associative:*
$$a *_2 (b *_2 c) = (a *_2 b) *_2 c, \forall a, b, c \in R$$
- *Identity: For any $a \in R$, there exists a unique $e_2 \in R$ such that,*
$$a *_2 e_2 = e_2 *_2 a = a$$
, then 'e_2' is called as an identity element of R w.r.t. $*_2$.
- *Distributive of $*_1$ over $*_2$:*
$a *_2 (b *_1 c) = (a *_2 b) *_1 (a *_2 c)$
$(a *_1 b) *_2 c = (a *_1 c) *_2 (b *_1 c)$

  When it satisfies the above mention properties, then it is called ring.
- *Commutative:*
$$a *_2 b = b *_2 a, \forall a, b \in G$$
When a Ring satisfies commutative property w.r.t. $*_2$, then we call $(R, *_1, *_2)$ as a **commutative ring with identity**

3.1 Integral Domain

Commutative ring that obeys the following axioms

- *Multiplicative identity: There is an element 1 in R such that a1=1a=a, $\forall a \in R$*
- *Non Zero divisors: If a, b in R and ab = 0, then either a = 0 or b=0.*

Example 3.1 *Check the following (Whether Ring or not)*

1. *The set of integers with usual addition and multiplication*
   Solution:- Set of integers with usual addition is an abelian group as shown above in example (2.1-1)
   For multiplication:

   - *Closure:*
     $$\forall a, b \in Z \Rightarrow a * b \in Z$$
   - *Associative:*
     $$a * (b * c) = (a * b) * c, \forall a, b, c \in Z$$
   - *Identity: For any $a \in Z$, there exists a unique $e_2 \in R$ such that,*
     $$a * 1 = 1 * a = a$$
     , then '1' is an identity element of Z w.r.t. $*$.
   - *Distributive of $+$ over $*$:*
     $a * (b + c) = (a * b) + (a * c)\ \forall a, b, c \in Z$
     $(a + b) * c = (a * c) + (b * c)\ \forall a, b, c \in Z$

     Therefore the set of integers with usual addition and multiplication is a ring.

2. *The set of real numbers with usual addition and multiplication*
   Solution:- Set of real numbers with usual addition is an abelian group as shown above in example (2.1-3)
   For multiplication:

   - *Closure:*
     $$\forall a, b \in R \Rightarrow a * b \in R$$
   - *Associative:*
     $$a * (b * c) = (a * b) * c, \forall a, b, c \in R$$
   - *Identity: For any $a \in R$, 1 is an identity element of R such that,*
     $$a * 1 = 1 * a = a$$
     .
   - *Distributive of $+$ over $*$:*
     $a * (b + c) = (a * b) + (a * c)\ \forall a, b, c \in R$
     $(a + b) * c = (a * c) + (b * c)\ \forall a, b, c \in R$

     Therefore the set of real numbers with usual addition and multiplication is a ring.

3. *The set of rational numbers with usual addition and multiplication*
Solution:- Let $a, b, c \in Q$, *then*
Closure Property:

$$a + b \in Q$$

Associative Property:

$$a + (b + c) = (a + b) + c, \forall a, b, c \in Q$$

Identity Property:

$$a + 0 = 0 + a = a, \forall a \in Q$$

Inverse Property:

$$a + \ (-a\ ) = \ (-a\ ) + a = 0, \forall a \in Q$$

Commutative Property:

$$a + b = b + a, \forall a, b \in Q$$

So, the set of rational numbers with usual addition is an abelian group.

For multiplication:

- *Closure:*
$$\forall a, b \in R \Rightarrow a * b \in Q$$
- *Associative:*
$$a * (b * c) = (a * b) * c, \forall a, b, c \in Q$$
- *Identity: For any* $a \in Q$, 1 *is an identity element of* Q *such that,*

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

.

- *Distributive of* $+$ *over* $*$*:*
$a * (b + c) = (a * b) + (a * c)\ \forall a, b, c \in Q$
$(a + b) * c = (a * c) + (b * c)\ \forall a, b, c \in Q$

Therefore the set of rational numbers with usual addition and multiplication is a ring.

4. *The set of Even integers(2N) with usual addition and multiplication*
Solution:-
Closure Property:

$$a + b \in 2N$$

Associative Property:

$$a + (b + c) = (a + b) + c, \forall a, b, c \in 2N$$

Identity Property:

$$a + 0 = 0 + a = a, \forall a \in 2N$$

Inverse Property:

$$a + \ (-a\ ) = \ (-a\ ) + a = 0, \forall a \in 2N$$

Commutative Property:

$$a + b = b + a, \forall a, b \in 2N$$

So, the set of even integers with usual addition is an abelian group.

For multiplication:

- *Closure:*
$$\forall a, b \in R \Rightarrow a * b \in 2N$$
- *Associative:*
$$a * (b * c) = (a * b) * c, \forall a, b, c \in 2N$$
- *Identity: For any $a \in Q$, 1 is an identity element of $2N$ such that,*
$$a * 1 = 1 * a = a$$
.
- *Distributive of $+$ over $*$:*
$a * (b + c) = (a * b) + (a * c)\ \forall a, b, c \in 2N$
$(a + b) * c = (a * c) + (b * c)\ \forall a, b, c \in 2N$

  Therefore the set of even integers with usual addition and multiplication is a ring.

4 Fields:-

Definition 4.1 *A set F with two Binary operations $*_1, *_2$ (denoted by $(F, *_1, *_2)$) is said to be a field, if it satisfies the following axioms,*

1. *$(F, *_1, *_2)$ is a commutative ring with identity*
   (a) *$(F, *_1)$ is an abelian group*
   (b) *Closure:*
   $$\forall a, b \in F \Rightarrow a *_2 b \in F$$
   (c) *Associative:*
   $$a *_2 (b *_2 c) = (a *_2 b) *_2 c, \forall a, b, c \in F$$
   (d) *Identity: For any $a \in F$, there exists a unique $e_2 \in F$ such that,*
   $$a *_2 e_2 = e_2 *_2 a = a$$
   , then 'e_2' is called as an identity element of F w.r.t. $*_2$.
   (e) *Distributive of $*_1$ over $*_2$:*
   $a *_2 (b *_1 c) = (a *_2 b) *_1 (a *_2 c)$
   $(a *_1 b) *_2 c = (a *_1 c) *_2 (b *_1 c)$
   (f) *Commutative:*
   $$a *_2 b = b *_2 a, \forall a, b \in F$$
2. *For every non-zero element $a \in F$, we must get a unique element $a' \in F$ such that, $a *_2 a' = a' *_2 a = e_2$.*

Example 4.1 *Check the following (Whether Field or not)*

1. *The set of integers with usual addition and multiplication*
   Solution:-
   Closure Property:
   $$a + b \in Z$$
   Associative Property:
   $$a + (b + c) = (a + b) + c, \forall a, b, c \in Z$$
   Identity Property:
   $$a + 0 = 0 + a = a, \forall a \in Z$$
   Inverse Property:
   $$a + (-a) = (-a) + a = 0, \forall a \in Z$$

Commutative Property:

$$a + b = b + a, \forall a, b \in Z$$

So, the set of integers with usual addition is an abelian group.

For multiplication:

- *Closure:*
$$\forall a, b \in Z \Rightarrow a * b \in Z$$
- *Associative:*
$$a * (b * c) = (a * b) * c, \forall a, b, c \in Z$$
- *Identity: For any $a \in Z$, 1 is an identity element of Z such that,*
$$a * 1 = 1 * a = a$$
.
- *Distributive of $+$ over $*$:*
$a * (b + c) = (a * b) + (a * c)\ \forall a, b, c \in Z$
$(a + b) * c = (a * c) + (b * c)\ \forall a, b, c \in Z$
- *Commutative:*
$$a * b = b * a \forall a, b \in Z$$
- *Multiplicative Inverse:*
$$a * a^{-1} = a^{-1} * a = 1, \forall a^{-1} \notin Z$$

Therefore the set of integers with usual addition and multiplication is not a field.

2. *The set of real numbers with usual addition and multiplication*
Solution:-
Closure Property:
$$a + b \in R$$

Associative Property:

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

Identity Property:

$$a + 0 = 0 + a = a, \forall a \in R$$

Inverse Property:

$$a + \ (-a\ ) = \ (-a\ ) + a = 0, \forall a \in R$$

Commutative Property:

$$a + b = b + a, \forall a, b \in R$$

So, the set of real numbers with usual addition is an abelian group.

For multiplication:

- *Closure:*
$$\forall a, b \in R \Rightarrow a * b \in R$$
- *Associative:*
$$a * (b * c) = (a * b) * c, \forall a, b, c \in R$$
- *Identity: For any $a \in R$, 1 is an identity element of R such that,*
$$a * 1 = 1 * a = a$$
.
- *Distributive of $+$ over $*$:*
$a * (b + c) = (a * b) + (a * c)\ \forall a, b, c \in R$
$(a + b) * c = (a * c) + (b * c)\ \forall a, b, c \in R$
- *Commutative:*
$$a * b = b * a \forall a, b \in R$$
- *Multiplicative Inverse:*
$$a * a^{-1} = a^{-1} * a = 1, \forall a^{-1} \in R$$

Therefore the set of real numbers with usual addition and multiplication is a field.

3. *The set of rational numbers with usual addition and multiplication*
Solution:-
Closure Property:

$$a + b \in Q$$

Associative Property:

$$a + (b + c) = (a + b) + c, \forall a, b, c \in Q$$

Identity Property:

$$a + 0 = 0 + a = a, \forall a \in Q$$

Inverse Property:

$$a + \ (-a\ ) = \ (-a\ ) + a = 0, \forall a \in Q$$

Commutative Property:

$$a + b = b + a, \forall a, b \in Q$$

So, the set of rational numbers with usual addition is an abelian group.

For multiplication:

- *Closure:*
$$\forall a, b \in Q \Rightarrow a * b \in Q$$
- *Associative:*
$$a * (b * c) = (a * b) * c, \forall a, b, c \in Q$$
- *Identity: For any $a \in Q$, 1 is an identity element of Q such that,*
$$a * 1 = 1 * a = a$$
.
- *Distributive of $+$ over $*$:*
$a * (b + c) = (a * b) + (a * c)\ \forall a, b, c \in Q$
$(a + b) * c = (a * c) + (b * c)\ \forall a, b, c \in Q$
- *Commutative:*
$$a * b = b * a \forall a, b \in Q$$

- *Multiplicative Inverse:*

$$a * a^{-1} = a^{-1} * a = 1, \forall a^{-1} \in Q$$

Therefore the set of rational numbers with usual addition and multiplication is a field.

4. *The set of Even integers with usual addition and multiplication*
Solution:-
Closure Property:

$$a + b \in 2N$$

Associative Property:

$$a + (b + c) = (a + b) + c, \forall a, b, c \in 2N$$

Identity Property:

$$a + 0 = 0 + a = a, \forall a \in 2N$$

Inverse Property:

$$a + \ (-a\ ) = \ (-a\ ) + a = 0, \forall a \in 2N$$

Commutative Property:

$$a + b = b + a, \forall a, b \in 2N$$

So, the set of even integers with usual addition is an abelian group.

For multiplication:

- *Closure:*

$$\forall a, b \in R \Rightarrow a * b \in 2N$$

- *Associative:*

$$a * (b * c) = (a * b) * c, \forall a, b, c \in 2N$$

- *Identity: For any $a \in Q$, 1 is an identity element of $2N$ such that,*

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

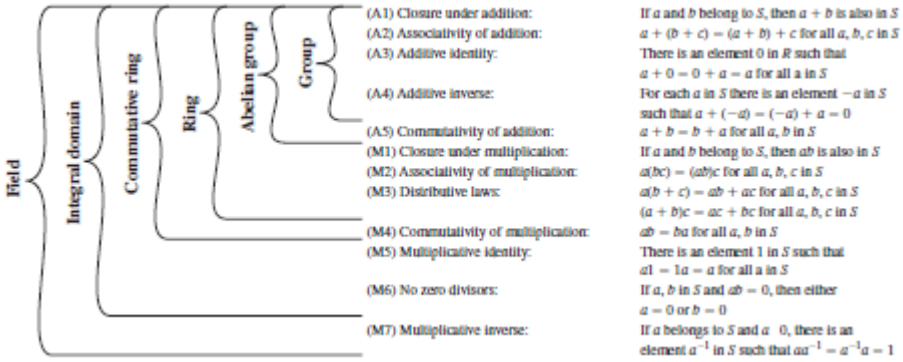
.

- *Distributive of + over ∗:*
  $a * (b + c) = (a * b) + (a * c)\ \forall a, b, c \in 2N$
  $(a + b) * c = (a * c) + (b * c)\ \forall a, b, c \in 2N$

- *Commutative:*
  $$a * b = b * a \forall a, b \in 2N$$

- *Multiplicative Inverse:*
  $$a * a^{-1} = a^{-1} * a = 1, \forall a^{-1} \notin 2N$$

  Therefore the set of even integers with usual addition and multiplication is not a field.



4.1 Finite Fields of the form GF(p)

- *Finite fields play a crucial role in many cryptographic algorithms.*
- *The order of a finite field (number of elements in the field) must be a power of a prime p^n , where n is a positive integer.*
- *The finite field of order p^n is generally written GF(p^n); GF stands for Galois field.*
- *For a given prime, p, we define the finite field of order p, GF(p), as the set Z_p of integers 0, 1, . . . , p - 1 together with the arithmetic operations modulo p.*
- *Any integer in Z_n has a multiplicative inverse if and only if that integer is relatively prime to n.*

- *If n is prime, then all of the nonzero integers in Z_n are relatively prime to n, and therefore there exists a multiplicative inverse for all of the nonzero integers in Z_n.*

- *For example:- Z_5=0,1,2,3,4*
  1 mod 5 = 1; 1 is multiplicative inverse of itself
  *(2*3) mod 5 = 1; 2 is multiplicative inverse of 3*
  *(3*2) mod 5 = 1; 3 is multiplicative inverse of 2*
  *(4*4)mod 5 = 1; 4 is multiplicative inverse of itself*

- *If a and b are relatively prime, then b has a multiplicative inverse modulo a. That is, if gcd(a, b) = 1, then b has a multiplicative inverse modulo a.*

- *Galois Field*

$$GF(P) = (Z_p, \oplus, \otimes)$$

  for $GF(2^n)$, we use irreducible polynomial

5 Polynomial arithmetic

5.1 Ordinary Polynomial Arithmetic

- A polynomial of degree n (integer $n \geq 0$) is an expression of the form

  f(x)= $a_n X^n + a_{n-1} X^{n-1} + a_{n-2} X^{n-2} + ... + a_0 = \sum_{i=0}^{n} a_i X^i$

- A zero-degree polynomial is called a constant polynomial and is simply an element of the set of coefficients. An nth-degree polynomial is said to be a monic polynomial if a_n=1.

5.2 Polynomial Arithmetic with Coefficients in Z_p

- When polynomial arithmetic is performed on polynomials over a field, then division is possible.

- Note:- this does not mean that exact division is possible. Within a field, given two elements and , the quotient a/b is also an element of the field. However, given a ring R that is not a field, in general, division will result in both a quotient and a remainder; this is not exact division.

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

(a) Addition

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

(b) Subtraction

$$\begin{array}{r} x^3+x^2 \quad +2 \\ \times\ (x^2-x+1) \\ \hline x^3+x^2 \quad +2 \\ -x^4-x^3 \quad -2x \\ \hline x^5+x^4 \quad +2x^2 \\ \hline x^5 \quad +3x^2-2x+2 \end{array}$$

(c) Multiplication

$$\begin{array}{r} \quad\quad\quad x+2 \\ x^2-x+1 \overline{)\ x^3+x^2 \quad +2} \\ \quad\quad x^3-x^2+x \\ \hline \quad\quad\quad 2x^2-x+2 \\ \quad\quad\quad 2x^2-2x+2 \\ \hline \quad\quad\quad\quad x \end{array}$$

(d) Division

5.3 Irreducible Polynomial

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

The polynomial[9] $f(x) = x^4 + 1$ over GF(2) is reducible, because

$$x^4 + 1 = (x + 1)(x^3 + x^2 + x + 1).$$

Consider the polynomial $f(x) = x^3 + x + 1$. It is clear by inspection that x is not a factor of $f(x)$. We easily show that $x + 1$ is not a factor of $f(x)$:

$$\begin{array}{r} x^2+x \\ x+1 \overline{)\ x^3 \quad +x+1} \\ \underline{x^3+x^2} \\ \quad x^2+x \\ \quad \underline{x^2+x} \\ \quad\quad 1 \end{array}$$

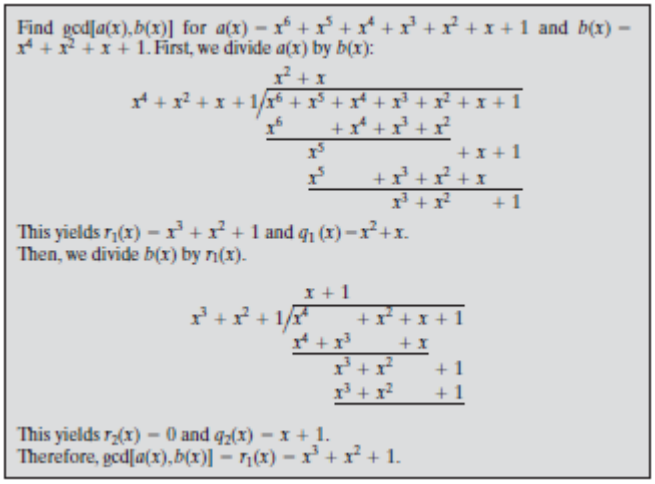
Thus, $f(x)$ has no factors of degree 1. But it is clear by inspection that if $f(x)$ is reducible, it must have one factor of degree 2 and one factor of degree 1. Therefore, $f(x)$ is irreducible.

5.4 Finding the Greatest Common Divisor

We can extend the analogy between polynomial arithmetic over a field and integer arithmetic by defining the greatest common divisor as follows.The polynomial is said to be the greatest common divisor of a(x) and b(x)if the following are true.

1. c(x) divides both a(x) and b(x).
2. Any divisor of a(x) and b(x) is a divisor of c(x).

We can adapt the Euclidean algorithm to compute the greatest common divisor of two polynomials.



6 Symmetric Cipher Model:-

A symmetric encryption scheme has five ingredients

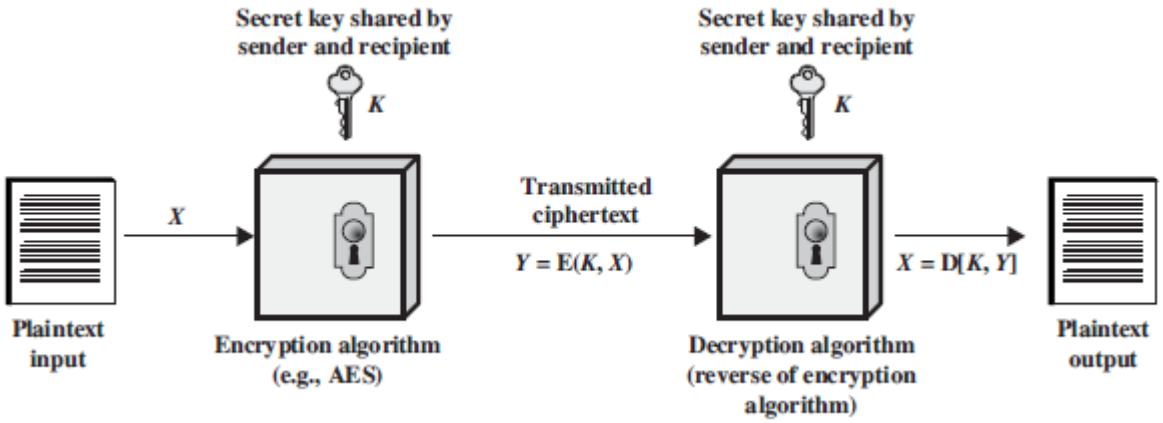
- Plaintext: This is the original intelligible message or data that is fed into the algorithm as input.
- Encryption algorithm: The encryption algorithm performs various substitutions and transformations on the plaintext.
- Secret key: The secret key is also input to the encryption algorithm.The key is a value independent of the plaintext and of the algorithm. The algorithm will produce a different output depending on the specific key being used at the time.The exact substitutions and transformations performed by the algorithm depend on the key.
- Ciphertext: This is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys

will produce two different ciphertexts. The ciphertext is an apparently random stream of data and, as it stands, is unintelligible.

- Decryption algorithm: This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext.

There are two requirements for secure use of conventional encryption:

1. We need a strong encryption algorithm.
2. Sender and receiver must have obtained copies of the secret key in a secure manner.



In Symmetric Cipher Model, we assume that it is impractical to decrypt a message on the basis of the ciphertext plus knowledge of the encryption/decryption algorithm. In other words,we do not need to keep the algorithm secret; we need to keep only the key secret.

6.1 Cryptography

Cryptographic systems are characterized along three independent dimensions:

1. The type of operations used for transforming plaintext to ciphertext.
2. The number of keys used.
3. The way in which the plaintext is processed.

6.2 Cryptanalysis and Brute-Force Attack

A brute-force attack involves trying every possible key until an intelligible translation of the ciphertext into plaintext is obtained.
In contrast to attacking via brute force, if the attacker has information about which keys are more likely than others and use such information to try and learn the key, then such attack becomes cryptanalysis.

7 Substitution Technique:-

The two basic building blocks of all encryption techniques are substitution and transposition.
In substitution technique we substitute plain text with other letters,symbols or numbers.
For Example:-
Plain Text: H E L L O
Key: 3
Cipher Text:K H O O R

1. Monoalphabetic Cipher :A monoalphabetic cipher is any cipher in which the letters of the plain text are mapped to cipher text letters based on a single alphabetic key. Examples of monoalphabetic ciphers would include the Caesar-shift cipher, where each letter is shifted based on a numeric key.

2. Polyalphabetic Cipher : A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets.

- Monoalphabetic Cipher : Caesar Cipher, Affine Cipher
- Polyalphabetic Cipher : Vigenère Cipher, Vernam Cipher

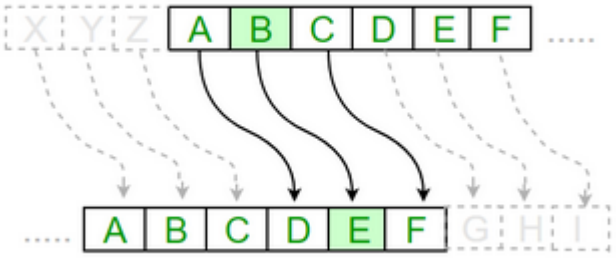
7.1 Caesar Cipher

The Caesar Cipher technique is one of the earliest and simplest method of encryption technique. It's simply a type of substitution cipher, i.e., each letter of a given text is replaced by a letter some fixed number of positions down the alphabet.
The encryption can be represented using modular arithmetic by first transforming the letters into numbers, according to the scheme, A = 0, B = 1,. . . , Z = 25.
Encryption of a letter by a shift n can be described mathematically as.

$$Encrption : E_n(x) = (x + n) mod 26$$

$$Decrption : D_n(x) = (x - n) mod 26$$

For Example: if key=3, then:



If it is known that a given ciphertext is a Caesar cipher, then a brute-force cryptanalysis is easily performed: simply try all the 25 possible keys.
Three important characteristics of Caesar Cipher enabled us to use a brute-force cryptanalysis:

1. The encryption and decryption algorithms are known.
2. There are only 25 keys to try.
3. The language of the plaintext is known and easily recognizable.

7.2 Affine Cipher:

The Affine cipher is a type of monoalphabetic substitution cipher, wherein each letter in an alphabet is mapped to its numeric equivalent, encrypted using a simple mathematical function, and converted back to a letter.

Encryption: It uses modular arithmetic to transform the integer that each plaintext letter corresponds to into another integer that correspond to a ciphertext letter. The encryption function for a single letter is
E (x) = (a x + b) mod m
modulus m: size of the alphabet
a and b: key of the cipher.
a must be chosen such that a and m are coprime.

Decryption: D (x) = a^{-1} (x - b) mod m a^{-1} : modular multiplicative inverse of a modulo m. i.e., it satisfies the equation 1 = a.a^{-1} mod m .

Encryption: Key Values a=17, b=20

Original Text	T	W	E	N	T	Y		F	I	F	T	E	E	N
x	19	22	4	13	19	24		5	8	5	19	4	4	13
ax+b % 26*	5	4	10	7	5	12		1	0	1	5	10	10	7
Encrypted Text	F	E	K	H	F	M		B	A	B	F	K	K	H

Decryption: a^-1 = 23

Encrypted Text	F	E	K	H	F	M		B	A	B	F	K	K	H
Encrypted Value	5	4	10	7	5	12		1	0	1	5	10	10	7
23 *(x-b) mod 26	19	22	4	13	19	24		5	8	5	19	4	4	13
Decrypted Text	T	W	E	N	T	Y		F	I	F	T	E	E	N

7.3 Vigenère Cipher

- The table consists of the alphabets written out 26 times in different rows, each alphabet shifted cyclically to the left compared to the previous alphabet, corresponding to the 26 possible Caesar Ciphers.
- At different points in the encryption process, the cipher uses a different alphabet from one of the rows.
- The alphabet used at each point depends on a repeating keyword.

Example 7.1 *Plaintext : GEEKSFORGEEKS*
Keyword : AYUSH
Ciphertext : GCYCZFMLYLEIM

Table to encrypt – Geeks

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

For generating key, the given keyword is repeated in a circular manner until it matches the length of the plain text.
The keyword "AYUSH" generates the key "AYUSHAYUSHAYU"
The plain text is then encrypted using the process explained below.
Encryption: The first letter of the plaintext, G is paired with A, the first letter of the key. So use row G and column A of the Vigenère square, namely G. Similarly, for others. Using Algebracially it can be as:
The plaintext(P) and key(K) are added modulo 26.
$E_i = (P_i + K_i) mod 26$
Decryption:
$D_i = (E_i - K_i + 26) mod 26$

7.4 Vernam Cipher:

In this mechanism we assign a number to each character of the Plain-Text, like (a = 0, b = 1, c = 2, ... z = 25).
Method to take key:
In Vernam cipher algorithm, we take a key to encrypt the plain text which length should be equal to the length of the plain text.
Encryption Algorithm:

- Assign a number to each character of the plain-text and the key according to alphabetical order.
- Add both the number (Corresponding plain-text character number and Key character number).
- Subtract the number from 26 if the added number is greater than 26, if it isn't then leave it.

Example 7.2 *Plain-Text: RAMSWARUPK*
Key: RANCHOBABA
PT: R A M S W A R U P K
NO: 17 0 12 18 22 0 17 20 15 10
KEY: R A N C H O B A B A
NO : 17 0 13 2 7 14 1 0 1 0
on adding Both:
CT-NO: 34 0 25 20 29 14 18 20 16 10
In this case, there are two numbers which are greater than the 26 so we have to subtract 26 from them and after applying the subtraction operation the new Cipher text character numbers are as follow:
CT-NO: 8 0 25 20 3 14 18 20 16 10
New Cipher-Text is after getting the corresponding character from the number.
CIPHER-TEXT: I A Z U D O S U Q K

7.5 Playfair Cipher

The Playfair Cipher Encryption Algorithm:
The Algorithm consistes of 2 steps:
Generate the key square(5*5)

- The key square is a 5*5 grid of alphabets that acts as the key for encrypting the plaintext. Each of the 25 alphabets must be unique and one letter of the alphabet (usually J) is omitted from the table (as the table can hold only 25 alphabets). If the plaintext contains J, then it is replaced by I.
- The initial alphabets in the key square are the unique alphabets of the key in the order in which they appear followed by the remaining letters of the alphabet in order.

Algorithm to encrypt the plain text: The plaintext is split into pairs of two letters

- If both the letters are in the same column: Take the letter below each one (going back to the top if at the bottom).
- If both the letters are in the same row: Take the letter to the right of each one (going back to the leftmost if at the rightmost position).
- If neither of the above rules is true: Form a rectangle with the two letters and take the letters on the horizontal opposite corner of the rectangle.

Example 7.3 *Using Key "monarchy"*

M	O	N	A	R
C	H	Y	B	D
E	F	G	I	K
L	P	Q	S	T
U	V	W	X	Z

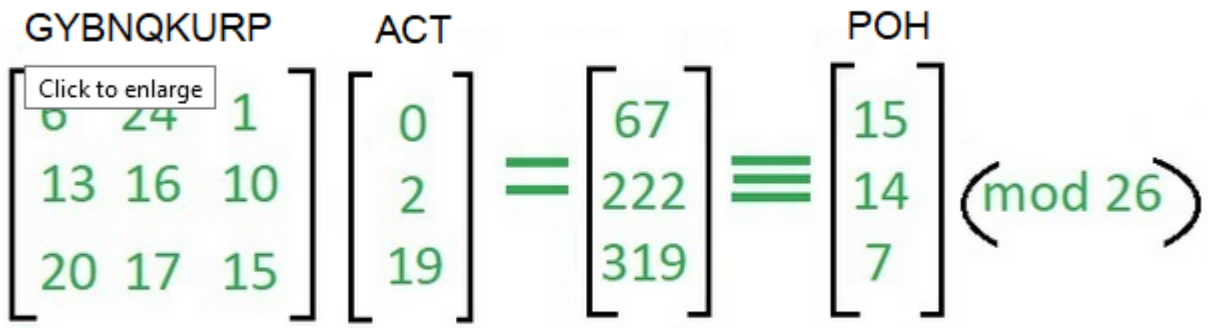
Plain Text: "instrumentsz"
Encrypted Text: gatlmzclrqtx
Encryption:
in: $i -> g$
$n -> a$
st: $s -> t$
$t -> l$
ru: $r -> m$
$u -> z$
me: $m -> c$
$e -> l$
nt: $n -> r$
$t -> q$
sz: $s -> t$
$z -> x$

7.6 Hill Cipher

Hill cipher is a polygraphic substitution cipher based on linear algebra.Each letter is represented by a number modulo 26. To encrypt a message, each block

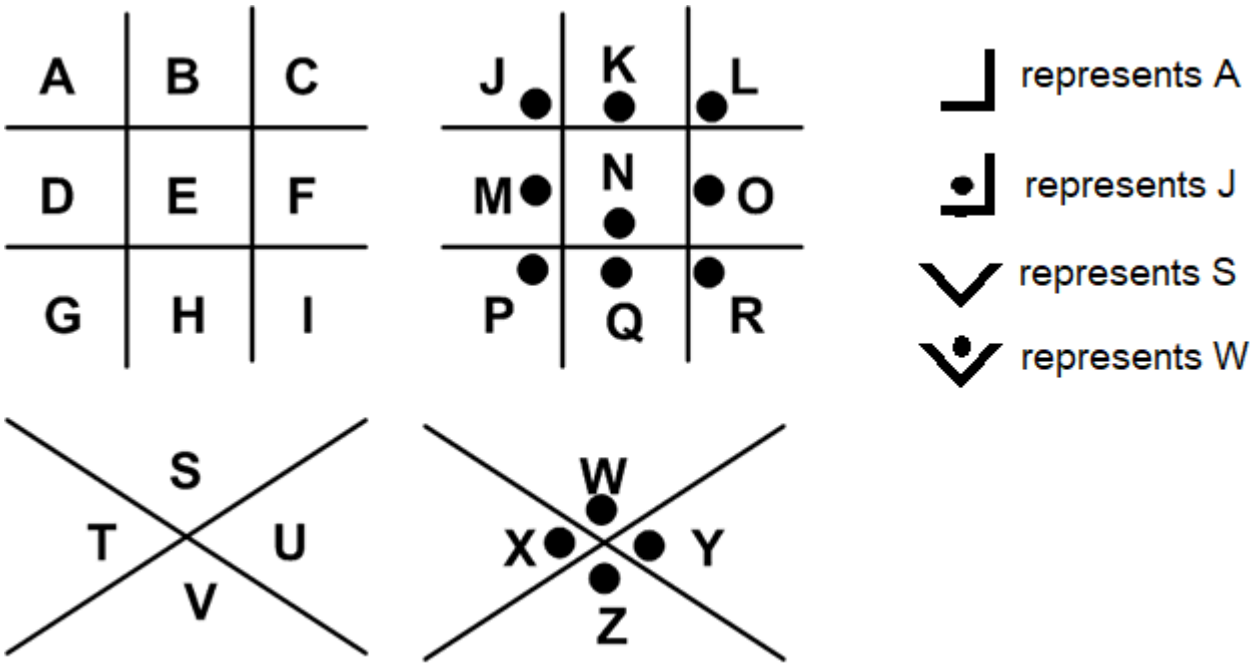
of n letters (considered as an n-component vector) is multiplied by an invertible n * n matrix, against modulus 26. To decrypt the message, each block is multiplied by the inverse of the matrix used for encryption.
The matrix used for encryption is the cipher key, and it should be chosen randomly from the set of invertible n * n matrices.

Example 7.4 *We have to encrypt the message 'ACT' (n=3).*
The key is 'GYBNQKURP'



7.7 Pigpen Cipher

The Pigpen Cipher is another example of a substitution cipher, but rather than replacing each letter with another letter, the letters are replaced by symbols.
Encryption:
The encryption process is fairly straightforward, replacing each occurence of a letter with the designated symbol. The symbols are assigned to the letters using the key shown below, where the letter shown is replaced by the part of the image in which it is located.



Decryption
The decryption process is just the reverse of the encryption process. Using the same key (the grid above), you locate the image depicted in the ciphertext, and replace it with the letter given by that part of the grid.

7.8 Enigma Machine

The Enigma machine is an encryption device developed and used in the early- to mid-20th century to protect commercial, diplomatic and military communication. It was employed extensively by Nazi Germany during World War II, in all branches of the German military.
Enigma has an electromechanical rotor mechanism that scrambles the 26 letters of the alphabet. In typical use, one person enters text on the Enigma's keyboard and another person writes down which of 26 lights above the keyboard lights up at each key press. If plain text is entered, the lit-up letters are the encoded ciphertext. Entering ciphertext transforms it back into readable plaintext. The rotor mechanism changes the electrical connections between the keys and the lights with each keypress. The security of the system depends on a set of machine settings that were generally changed daily during the war, based on secret key lists distributed in advance, and on other settings that were changed for each message. The receiving station has to know and use the exact settings employed by the transmitting station to successfully decrypt a message.

8 Transposition Technique

A very different kind of mapping is achieved by performing some sort of permutation on the plaintext letters. This technique is referred to as a transposition cipher.

8.1 Rail Fence Cipher

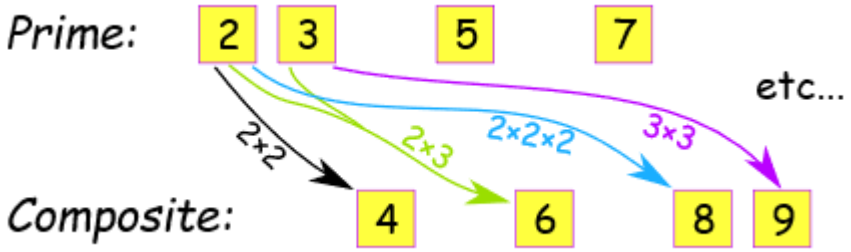
The rail fence cipher (also called a zigzag cipher) is a form of transposition cipher. It derives its name from the way in which it is encoded.
Encryption
Input : "attack at once"
Key = 2
Output : atc toctaka ne
Decryption
Input : "atc toctaka ne"
Key = 2
Output : attack at once

9 Steganography

Steganography is the technique of hiding secret data within an ordinary, non-secret, file or message in order to avoid detection; the secret data is then extracted at its destination. The use of steganography can be combined with encryption as an extra step for hiding or protecting data.

10 Fundamental Theorem of Arithmetic:

The fundamental theorem of arithmetic states that every positive integer (except the number 1) can be represented in exactly one way apart from rearrangement as a product of one or more primes.
This theorem is also called the unique factorization theorem. The fundamental theorem of arithmetic is a corollary of the first of Euclid's theorems.



11 Euler's Totient Function:

Euler's totient function, also known as phi-function $\phi(n)$, counts the number of integers between 1 and n inclusive, which are co-prime to n. Two numbers are co-prime if their greatest common divisor equals 1.
Here are values of $\phi(n)$ for the first few positive integers:

n	1	2	3	4	5	6	7	8	9	10	11	12	13
$\phi(n)$	1	1	2	2	4	2	6	4	6	4	10	4	12

11.1 Properties:

The following properties of Euler totient function are sufficient to calculate it for any number:

- If p is a prime number, then GCD(p,q) = 1, $\forall 1 \leq q < p$.
  Therefore we have: $\phi(p) = p - 1$
- If a and b are relatively prime, then:
  $\phi(pq) = \phi(p) * \phi(q) = (p-1)(q-1)$
- If p is a prime number and $k \geq 1$, then there are exactly p^k/p numbers between 1 and p^k that are divisible by p. Which gives us:

$$\phi(p^k) = p^k - p^{k-1}$$

12 Fermat's Little theorem:

Fermat's little theorem is a fundamental theorem in elementary number theory, which helps compute powers of integers modulo prime numbers.
Let p be any prime number and a be any integer. Then a^p-p is always divisible by p.
Modular arithmetic notation: $a^p \equiv$ a mod p
$a^{p-1} \equiv 1$ mod p
For example: a = 7, p = 19
$7^2 = 49 = 11(\text{mod } 19)$
$7^4 = 121 = 7(\text{mod } 19)$
$7^8 = 49 = 11(\text{mod } 19)$
$7^{16} = 121 = 7(\text{mod } 19)$
$a^{p-1} = 7^{18} = 7^{16} * 7^2 = 7*11 = 1(\text{mod } 19)$

13 System of Linear Congruences

1. Using solution sets.
2. Using equations.

3. Chinese Remainder Theorem (C.R.T)

13.1 Using solution sets:

x = 1 mod 3
x = 3 mod 5
A1 = ..., -2, 1, 4, 7, 10,...
A2 = ..., -2, 3, 8, 13, 18,...
solution set for x = A1 ∩ A2

13.2 Using Equation:

x ≡ 3 mod 5
x ≡ 1 mod 3
x=5q1 + 3 ..eq(1)
x=3q2 + 1 ..eq(2)
5q1 = 3q2 - 2
5q1 mod 3 = 1 mod 3
q1 5*2 mod 3 = 2 mod 3
q1 = 3k +2
using eq(1):
x = 5q1 + 3
x = 5(3k + 2) +3
x = 15k + 13

13.3 Chinese Remainder Theorem (C.R.T)

Chinese remainder theorem gives us an algorithm for solving a system of linear congruences with one unknown.
Proof:
$M = m_1 * m_2 * m3 * ... * m_r$ and $M_j = M/m_j$, for j = 1 to r
Let $y_i$be an inverse of M_j modulo m_j
Then , x = $\sum_1^r a_j M_j y_j$ Mod M
For Example:
x ≡ a1 mod n1
x ≡ a2 mod n2
x ≡ a3 mod n3
M = a1*a2*a3
m1 = M/a1
m2 = M/a2
m3 = M/a3
y1 = $(m1^{-1})$ Mod a1
y2 = $(m2^{-1})$ Mod a2
y3 = $(m3^{-1})$ Mod a3
x = $\sum_1^3 a_i M_i y_i$ Mod M

14 RSA Algorithm:

RSA algorithm is asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys i.e. Public Key and Private Key. As the name describes that the Public Key is given to everyone and Private key is kept private.
The idea of RSA is based on the fact that it is difficult to factorize a large integer. The public key consists of two numbers where one number is multiplication of two large prime numbers. And private key is also derived from the same two prime numbers. So if somebody can factorize the large number, the private key is compromised. Therefore encryption strength totally lies on the key size and if we double or triple the key size, the strength of encryption increases exponentially. RSA keys can be typically 1024 or 2048 bits long, but experts believe that 1024 bit keys could be broken in the near future. But till now it seems to be an infeasible task.

14.1 Algorithm:

- Step 1: Choose large p,q
- Step 2: n = p.q
- Step 3: Choose e: $1 < e < \phi(n)$
- Step 4: Calculate d: d = e^{-1} Mod $\phi(n)$
- Step 5: Public Key (e,n)
  Priavte Key (d,p,q) - secret key
  $\phi(n)$ = (p-1)*(q-1)
- Step 6: C = M^e Mod n
  M = C^d Mod n

15 Quadratic Residue Mod p

If there is an integer $0 < x < p$ such that
$x^2 = q$(mod p)
the congruence has a solution, then q is said to be a quadratic residue (mod p).Note that the trivial case q=0 is generally excluded from lists of quadratic residues so that the number of quadratic residues (mod n) is taken to be one less than the number of squares (mod n). However, other sources include 0 as a quadratic residue.
If the congruence does not have a solution, then q is said to be a quadratic non-residue (mod p).
In practice, it suffices to restrict the range to $0 < x <= \lfloor p/2 \rfloor$, where $\lfloor x \rfloor$ is the floor function, because of the symmetry $(p - x)^2 = x^2$ (mod p).
For Example: Z_7=0,1,2,3,4,5,6

1^2 Mod 7 = 1
2^2 Mod 7 = 4
3^2 Mod 7 = 2
4^2 Mod 7 = 2
5^2 Mod 7 = 4
6^2 Mod 7 = 1
Q R Mod P = 1,2,4
x1 = r then x2 = -r + p
For Quadratic Non-Residue Mod p
No. of QNR_p Mod p $\Rightarrow$ (p-1)/2
No. of QR_p Mod p $\Rightarrow$ (p-1)/2

16 Euler's Criterion :

Let p be a prime number, then for any x $\in Z_p^*$, x $\in$ QR Mod p,iff
$a^{(p-1)/2} = 1$ Mod p
For Example: Let p = 29 and a = 13
$13^{(29-1)/2} \equiv 13^{14}$
13 Mod 29 = 13
13^2 Mod 29 = 24
13^4 Mod 29 = 24^2 Mod 29 = 25
13^8 Mod 29 = 25^2 Mod 29 = 16
16*25*24 Mod 29 $\equiv$ 9600 Mod 29 $\equiv$ 1

17 Legendre Symbol :

Legendre Symbol is defined to be equal to ± 1 depending on whether 'a' is a quadratic residue modulo p.

$$\left(\frac{a}{p}\right) = (a \mid p) \equiv \begin{cases} 0 & \text{if } p \mid a \\ 1 & \text{if } a \text{ is a quadratic residue modulo } p \\ -1 & \text{if } a \text{ is a quadratic nonresidue modulo } p. \end{cases}$$

For Example:
(169/13) = 0
(2/13) = -1
$2^{(13-1)/2}$ Mod 13
2^6 Mod 13
64 Mod 13

18 Jacobi Symbol :

The Jacobi symbol is a generalization of the Legendre symbol, which can be used to simplify computations involving quadratic residues. It shares many of the properties of the Legendre symbol, and can be used to state and prove an extended version of the law of quadratic reciprocity.
Jacobi Symbol (JS) ⇒ Legendre Symbol (LS)
Legendre Symbol (LS) doesn't implies Jacobi Symbol

The Jacobi symbol, written (n/m) or $\left(\frac{n}{m}\right)$ is defined for positive odd m as

$$\left(\frac{n}{m}\right) = \left(\frac{n}{p_1}\right)^{a_1} \left(\frac{n}{p_2}\right)^{a_2} \cdots \left(\frac{n}{p_k}\right)^{a_k},$$

where

$$m = p_1^{a_1} \ p_2^{a_2} \cdots p_k^{a_k}$$

P_k is distinct prime nos.
(a/n) = $\sum_1^k (a/P_i)^{ei}$

Primality test can be classified into

1. Deterministic (prime with 100 percent true)
2. Probablistic (Composite then 100 percent true, prime then may or may not be true)

To check prime (Primality Test)

1. Sieve of Eratosthenes
2. Square Root Method
3. Mersenne Prime
4. Fermat's Prime
5. Solovay strassen Algorithm
6. Miller-Rabin Primality Test

19 Sieve of Eratosthenes:

The sieve of Eratosthenes is one of the most efficient ways to find all primes smaller than n.
Steps to find all the prime numbers less than or equal to a given integer n by the Eratosthene's method:

1. Create a list of consecutive integers from 2 to n: (2, 3, 4, . . . , n).

2. Initially, let p equal 2, the first prime number.

3. Starting from p^2, count up in increments of p and mark each of these numbers greater than or equal to p^2 itself in the list. These numbers will be p(p+1), p(p+2), p(p+3), etc..

4. Find the first number greater than p in the list that is not marked. If there was no such number, stop. Otherwise, let p now equal this number (which is the next prime), and repeat from step 3.

20 Fermat Primality Test:

1. Add odd integer, n > 0

2. Choose random 'a', $\exists$ a < n

3. If the GCD(a,n) $\neq 1$
   Then n - not prime.

4. If a^{n-1} MOD n $\neq 1$
   Then n - composite.

5. If a^{n-1} MOD n = 1
   Then n - may be prime.

Example 20.1 *a = 4, n = 15*
a^{n-1} *= 1 MOD 15*
4^1 *= 4 MOD 15*
4^2 *= 1 MOD 15*
4^4 *= 1 MOD 15*
4^8 *= 1 MOD 15*
$4^{14} = 4^{2+4+8}$ *= 1 MOD 15*

21 Square Root Test:

Using Q.R MOD p
x^2 = a MOD p
$\sqrt{a}$ = +x, -x+p

Example 21.1 *3 in* Z_7
1^2 *MOD 7 = 1*
2^2 *MOD 7 = 4*
3^2 *MOD 7 = 2*
4^2 *MOD 7 = 2*
5^2 *MOD 7 = 4*
6^2 *MOD 7 = 1*

Square root of 1 MOD n is ± 1.
Square root of 1 MOD n is ± 1 , ± r, n is integer
P-primes ⟶ 6n ± 1 For numbers greater than 3.

22 Solovay strassen Algorithm:

1. Start with an odd positive integer n.
2. Choose a random integer 'a' such that 1 ¡ a ¡ n-1.
3. If GCD(a,n) ± 1, then n composite.
4. Find x = (a/n)
5. Calculate j = $a^{(n-1)/2}$ MOD n
6. If j ± (a/n), then n is not prime.
7. If j = (a/n), then n may be prime.

Example 22.1 *n=15, a= 4*

1. *n = 15*
2. *a = 4*
3. *GCD(4,15) = 1*
4. *x = 4/15*
5. *j* = $4^{14/2}$ *MOD 15*
   j = 4^{7} *MOD 15*
   j = 4
6. *j* ≠ *x. So, not prime*

23 Miller Rabin Primality Test

Choose an odd integer n.

1. Find integer k,q with k ¿ 0, q ∈ odd such that n-1 = 2^kq
2. Select random integer a, such that a ∈ (1,n-1)
3. If a^qMod n = 1, then return "inconclusive".
4. Else for j=1 to k-1 do
   if $a^{2^j q}$ MOD n = n-1 then return "Conclusive"
   else return Composite

Example 23.1 *n=29*
1. n-1=28=2^2*.7*
k=2,q=7
2. Let a = 10, (1¡a¡28)
3. a^q *Mod n:* 10^7 *Mod 29=17*
n-may be prime

24 Carmicheal Number

pseudo prime
It is nothing a composite number 'n' that satisfies:
n $\rightarrow p^{n-1} \equiv$ b MOD n
$\forall$ b,GCD(b,n) = 1
n-1 = $\pi\ p_i^{e_i}$ = (n-1)/(p-1)

25 Factorization Algorithm

25.1 Pollard P-1 Factoring Algorithm

```
1     Given a number n.
2     Initialize a = 2, i = 2
3     Until a factor is returned do
4     a <- (a^i) mod n
5     d <- GCD(a-1, n)
6     if 1 < d < n then
7         return d
8     else
9         i <- i+1
10    Other factor, d' <- n/d
11    If d' is not prime
12        n <- d'
13        goto 1
14    else
15        d and d' are two prime factors.
```

In this algorithm, the power of 'a' is continuously raised until a factor, 'd', of n is obtained. Once d is obtained, another factor, 'd", is n/d. If d' is not prime, the same task is repeated for d'.

25.2 Pollard Rho factorizing Algorithm:

1. Start with random x and c. Take y equal to x and $f(x) = x^2 + c$.
2. While a divisor isn't obtained
    1. Update x to f(x) (modulo n) [Tortoise Move]
    2. Update y to f(f(y)) (modulo n) [Hare Move]
    3. Calculate GCD of |x-y| and n
    4. If GCD is not unity
        1. If GCD is n, repeat from step 2 with another set of x, y and c
        2. Else GCD is our answer