Unit-V

~~Fields~~ Elementary number theory & Cryptography.

Group, Rings & fields

Algebraic structures

The set of elements & algebraic structure

Common algebraic structure

- Groups
- Rings
- fields

Group: A group G is a set of elements with binary operation (·) that satisfies four properties (or axioms). A commutative group satisfies an extra property, commutativity.

i) closure: $\forall a, b \in G$ we have $a \cdot b \in G$

ii) associativity: $\forall a, b, c \in G$ we have

$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$

iii) Existence of identity: $\exists$ an element $e \in G$ called the identity of the group such that

$$e \cdot a = a \cdot e = a \quad \forall a \in G$$

iv) Existence of inverse: $\forall a \in G$, $\exists$ a unique element $b \in G$ called the inverse of a such

$$a \cdot b = b \cdot a = e$$

Ex:- $G = \langle Z_n, + \rangle$

Ring: A ring $R = \langle \{\}, \bullet, \square \rangle$ is an algebraic structure with two operations.

distribution of $\square$ over $\bullet$

- $\bullet$
  - i) closure
  - ii) associativity
  - iii) commutativity
  - iv) Existence of identity
  - v) Existence of inverse
- $\square$
  - i) closure
  - ii) Associativity
  - iii) commutativity

(2) If it includes commutative property then it is called as commutative ring

Ex:- $G = \langle Z_n, +, \times \rangle$

Field:- A field denoted by $F = \langle \{ \ldots \}, \cdot, \square \rangle$ is a commutative ring in which the second operation satisfies all five properties defined for the first operation except that the identity of the first operation has no inverse

Distribution of $\square$ over $\cdot$

i) closure	i) closure
ii) Associativity	ii) Associativity
iii) Commutativity	iii) Commutativity
iv) Existence of identity	iv) Existence of identity
v) Existence of inverse	v) Existence of inverse.

Note :- For the multiplication the inverse as such does not exist for 0

Additive group of integers modulo n

Let K.T the relation "congruence modulo n" is an equivalence relation on $\mathbb{Z}$. Consequently this relation induces a partition of $\mathbb{Z}$ with the congruence classes as cells of the partition

$a \in Z$, the congruence class determined by a is given by the expression

$$[a] = \{x \in Z \mid x \equiv a \pmod{n}\}$$
$$= \{a + nx \mid x \in Z\}$$

Accordingly, we have

$$[0] = \{0 + nx \mid x \in Z\}$$
$$[1] = \{1 + nx \mid x \in Z\}$$
$$\vdots$$
$$[n-1] = \{(n-1) + nx \mid x \in Z\}$$

Let Z_n denote the set of all these n congruence classes:

$$Z_n = \{[0], [1], [2], \ldots [n-1]\}$$

let us define the operation "addition modulo n", denoted by $\oplus_n$, by $[x] \oplus [y] = [x+y]$ for all $[x], [y] \in Z_n$.

$[0]$ is identity element under $\oplus_n$.
and $-[x] = [n-x]$ is the inverse of any $[x] \in Z_n$ under $\oplus_n$.

$(Z_n, \oplus_n)$

the operation table for $(Z_6, \oplus_6)$

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Multiplicative group of Integers mod p.

Let n be a given integer ≥ 1, and Z_n denote the set of all congruence classes modulo n:

$$Z_n = \{[1], [2], [3], \ldots, [n-1]\}$$

Let us define the operation "multiplication modulo n", denoted by $\otimes_n$, by

$$[x] \otimes_n [y] = [x \times y], \text{ for all } [x], [y] \in Z_n$$

The elements of the group $(Z_p^*, \otimes_p)$ are denoted by $1, 2, 3, \ldots, p-1$. and the operation $\otimes_p$ by $\times$ or $\cdot$.

The operation table $(Z_7^*, \cdot)$ is given below

$\cdot$	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

Divisors

We say that a nonzero b divides a if $a = mb$ for some m. In other words b divides a if it leaves no remainder.

$b \mid a$ means b divides a.

Positive divisors of 18 are 1, 2, 3, 6, 9, 18.

If $a \mid 1$ then $a = \pm 1$. $a \mid b$ & $b \mid a \Rightarrow a = \pm b$.

$b \mid 0$ for any $b \neq 0$. $b \mid g$ & $b \mid h$ then $b \mid (mg + nh)$

Properties of Modulo Operator

1) $a \equiv b \pmod{n}$ mean $n \mid (a-b)$
2) $a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$
3) $a \equiv b \pmod{n}$ & $b \equiv c \pmod{n}$ then $a \equiv c \pmod{n}$.

Modular Arithmetic operations

Under division rule n maps all integers into a finite set $\{0, 1, 2, \ldots, n-1\}$ [remainders obtained on division by n].

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

① To find $11^7 \bmod 13$, $11^2 = 121 \equiv 4 \pmod{13}$

$11^4 \equiv 4^2 \equiv 3 \pmod{13}$ $11^7 = 11 \times 4 \times 3 \equiv 132 \equiv 2 \pmod{13}$.

Define $Z_n = \{0, 1, 2, \ldots, (n-1)\}$ set of nonnegative integers less than n. It's also called residue class modulo n. Each integer represents a set (residue class)

$$[r] = \{a : a \text{ integer}, a \equiv r \pmod{n}\}$$

For $n=4$, $Z_4 = \{0, 1, 2, 3\}$

$[0] = \{\ldots, -16, -12, -8, -4, 0, 4, 8, \ldots\}$

$[1] = \{\ldots -15, -11, -7, -3, 1, 5, 9, 13, \ldots\}$

$[2] = \{\ldots, -14, -10, -6, -2, 2, 6, 10, 14\}$

$[3] = \{\ldots -13, -9, -5, -1, 3, 7, 11, 15, 19\}$

Of all the integers in a residue class, the smallest nonnegative integer is the one usually used to represent the residue class. Finding the smallest nonnegative integer to which k is congruent modulo n is called reducing k modulo n.

If $(a+b) \equiv (a+c) \bmod n$ then $b \equiv c \pmod{n}$

Ex: $(5+23) \equiv (5+7) \bmod 8$. $23 \equiv 7 \pmod 8$

* If $a \cdot b \equiv a \cdot c \bmod n$ then $b \equiv c \pmod n$ if a is relatively prime to n.

Ex: $6 \times 3 \equiv 2 \pmod 8$ & $6 \times 7 \equiv 2 \pmod 8$
but $3 \not\equiv 7 \pmod 8$ as 6 & 8 are not relatively prime

Two integers are relatively prime if their only common positive integer factor is 1.

Eg: $(8, 11) = 1$, $(15, 17) = 1$, $(9, 23, 19) = 1$.

Greatest Common Divisor

The positive integer c is said to be the greatest common divisor of a and b. if

1) c is a divisor of a and of b;
2) any divisor of a and b is a divisor of c.

This is denoted by $\gcd(a, b)$

equivalently. $\gcd(a,b) = \max[k, \Rightarrow k|a \text{ and } k|b]$

$\gcd(a,b) = \gcd(a,-b) = \gcd(-a,b) = \gcd(-a,-b)$.

In general $\gcd(a,b) = \gcd(|a|,|b|)$.

$\gcd(60,24) = \gcd(60,-24) = 12$.

NOTE: $\gcd(a,0) = |a|$.

Thm: For any nonnegative integer a and any positive integer b,

$$\gcd(a,b) = \gcd(b, a \bmod b)$$

$\gcd(55,22) = \gcd(22, 55 \bmod 22) = \gcd(22,11) = 11$

Euclid's algorithm to find gcd of two numbers.

The algorithm assumes $a > b > 0$. It is acceptable to restrict the algorithm to positive integers ∵ $\gcd(a,b) = \gcd(|a|, |b|)$.

EUCLID (a, b)

1. $A \leftarrow a$, $B \leftarrow b$
2. if $B = 0$ return $A = \gcd(a, b)$
3. $R = A \bmod B$
4. $A \leftarrow B$
5. $B \leftarrow R$
6. goto 2.

Ex① To find gcd (1970, 1066)

$1970 = 1 \times 1066 + 904$ — gcd (1066, 904)
$1066 = 1 \times 904 + 162$ — gcd (904, 162)
$904 = 5 \times 162 + 94$ — gcd (162, 94)
$162 = 1 \times 94 + 68$ — gcd (94, 68)
$94 = 1 \times 68 + 26$ — gcd (68, 26)
$68 = 2 \times 26 + 16$ — gcd (26, 16)
$26 = 1 \times 16 + 10$ — gcd (16, 10)
$16 = 1 \times 10 + 6$ — gcd (10, 6)
$10 = 1 \times 6 + 4$ — gcd (6, 4)
$6 = 1 \times 4 + 2$ — gcd (4, 2)
$4 = 2 \times 2 + 0$ — gcd (2, 0)

∴ gcd (1970, 1066) = 2.

H.W① Find gcd (4655, 12075) = ? using Euclid's algorithm

Q) S.T GF(5) is a finite field on the set Z_5 (3)
(Z_5 is prime)

GF(5) = {0, 1, 2, 3, 4}

$\oplus_5$	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

→ Addition modulo 5

Multiplication modulo 5

$\otimes_5$	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

Additive & multiplicative inverse of modulo 5

w	$-w$	w^{-1}
0	0	–
1	4	1
2	3	3
3	2	2
4	1	4

∴ GF(5) is a finite field over Z_5

9) Show that GF(7) is a finite field

GF(7) = {0, 1, 2, 3, 4, 5, 6}

Addition modulo 7

$\oplus_7$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

multiplication modulo 7

$\otimes_7$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Additive → $-\omega$; multiplicative inverse of modulo 7 → ω^{-1}

ω	$-\omega$	ω^{-1}
0	0	—
1	6	1
2	5	4
3	4	5
4	3	2
5	2	3
6	1	6

∴ GF(7) is a finite field

polynomial arithmetic with co-efficients in Z_p

when polynomial arithmetic is performed in polynomials over a field then division is possible. It may result into some remainder also.

For the co-efficient set as set of integers $5x^2/3x$ does not have a solution as $5/3 \notin Z_p$ but over Z_{p7} its possible as

$$\frac{5}{3}\frac{x^2}{x} = \frac{5}{3}x = 5(3^{-1})\cdot x = 5\cdot 5x$$

↳ Refer ex GF(7) (inverse of 3 is 5)

$$= 4x \pmod 7$$

$\because 5\cdot 5 = 25$

$25 \equiv 4 \pmod 7$

*** A polynomial $f(x)$ over a field F is called irreducible iff $f(x)$ cannot be expressed as a product of two polynomial of lower degree. Its called as prime polynomial also

Ex: $x^4+1 = (x+1)(x^3+x^2+x+1)$ — reducible

x^3+x^2+1 - irreducible over GF(2).

If $a(x)$ & $b(x)$ are two polynomials then a polynomial $c(x)$ is said to be the greatest common divisor of $a(x)$ & $b(x)$ if

i) $c(x)$ divides $a(x)$ & $b(x)$

ii) any divisor of $a(x)$ & $b(x)$ is a divisor of $c(x)$

$\therefore \gcd[a(x), b(x)] = \gcd[b(x), a(x) \bmod b(x)]$

1) Find gcd [a(x), b(x)] for

$a(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ & $b(x) = x^4 + x^2 + x + 1$ in GF(2)

$$x^4+x^2+x+1 \;\overline{)\; x^6+x^5+x^4+x^3+x^2+x+1}$$

$x^2 + x$

$x^6 + x^4 + x^3 + x^2$

$x^5 + x + 1$

$x^5 + x^3 + x^2 + x$

$x^3 + x^2 + 1$

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

$x + 1$

$x^4 + x^3 + x$

$x^3 + x^2 + 1$

$x^3 + x^2 + 1$

0

$\therefore \gcd[a(x), b(x)] = x^3 + x^2 + 1$

2) Find gcd [a(x), b(x)] for

$a(x) = x^3 + x + 1$ & $b(x) = x^2 + x + 1$ over GF(2)

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

x

$x^3 + x^2 + x$

$x^2 + 1$

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

1

$x^2 + 1$

x

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

x

x^2

1

$\therefore \gcd[a(x), b(x)] = 1$

GF(2^n) Fields

In cryptography, we often need to use four operations (addition, substraction, multiplication & division). In other words, we need to use fields we can work in GF(2^n) & use a set of 2^n elements. The elements in this set are n-bit words

Ex: let us define GF($2^{**}2$) field in which the set has four 2 bit words ie {00, 01, 10, 11}. we can redefine addition & multiplicatn for this field in such a way that all properties of these operation are satisfied.

⊕	00	01	10	11
00	00	01	10	11
01	01	00	11	10
10	10	11	00	01
11	11	10	01	00

Identity: 00

⊗	00	01	10	11
00	00	00	00	00
01	00	01	10	11
10	00	10	11	01
11	00	11	01	10

Identity: 01

```
 01
×01
----
 01
 00
----
 01
```

Polynomials

A polynomial of degree n-1 is of the form

$f(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \dots + a_1x^1 + a_0x^0$

where x^i is called the ith term & a_i is called co-efficient of the ith term

Ex: Representation of an 8-bit word by a polynomial

n-bit word: 1 0 0 1 1 0 0 1

polynomial: $1x^7 + 0x^6 + 0x^5 + 1x^4 + 1x^3 + 0x^2 + 0x + 1$

1st simplifn: $1x^7 + 1x^4 + 1x^3 + 1x^0$

2nd n: $x^7 + x^4 + x^3 + 1$

Ex:- To find 8 bit word to the poly. $x^5 + x^2 + x^0$.

∵ n=8 it means polynomial is of degree 7

∴ $0x^7 + 0x^6 + 1x^5 + 0x^4 + 0x^3 + 1x^2 + 1x + 0x^0$

∴ the related 8 bit word is 00100110

(b) GF(2^n) Fields

polynomial representing n-bit words use two fields GF(2) & GF(2^n)

Note : Since 2^n is not a prime no. ($n>1$)
∴ we have the concept of prime polynomial or irreducible polynomial as a modulus

Modulus

For the sets of polynomial in GF(2^n) a group of polynomial of degree n is defined as the modulus such polynomial are refered to as irreducible polynomial.

degree	irreducible polynomial
1	$x, (x+1)$
2	x^2+x+1
3	$(x^3+x^2+1), (x^3+x+1)$
4	$(x^4+x^3+x^2+x+1), (x^4+x^2+1), (x^4+x+1)$
5	

Addition & substraction operations on polynomials are the same operation

Q) Show the addition & multiplication tables for the field GF(2^3)

GF(2^3) has 8 elements,

There are two irreducible polynomial ~~for~~ of degree 3 those are (x^3+x^2+1) & (x^3+x+1).
We will use irreducible polynomial (x^3+x^2+1)

** Note The irreducible polynomial x^3+x^2+1 yields totally different table for multiplicat

Addition table for GF(2^3)

⊕	0 000	1 001	x 010	x+1 011	x^2 100	x^2+1 101	x^2+x 110	x^2+x+1 111
000 (0)	000 0	001 1	010 x	011 x+1	100 x^2	101 x^2+1	110 x^2+x	111 x^2+x+1
001 (1)	001 (1)	000 (0)	011 x+1	010 x	101 x^2+1	100 x^2	111 x^2+x+1	110 x^2+x
010 (x)	010	011	000	001	010	111	100	101
011 (x+1)	011	010	001	000	111	110	101	100
100 (x^2)	100	101	110	111	000	001	010	011
101 (x^2+1)	101	100	111	110	001	000	011	010
110 x^2+x	110	111	100	101	010	011	000	001
111 x^2+x+1	111	110	101	100	011	010	001	000

Multiplication table for GF(2^3)

⊗	000 (0)	001 (1)	010 (x)	011 (x+1)	100 (x^2)	101 x^2+1	110 x^2+x	111 x^2+x+1
000 (0)	000 (0)	000 (0)	000 (0)	000 (0)	000 (0)	000 (0)	000 (0)	000 (0)
001 (1)	000	001	010	011	100	101	110	111
010 (x)	000	010	100	110	101	111	001	011
011 (x+1)	000	011	110	101	001	010	111	100
100 (x^2)	000	100	101	001	111	011	010	110
101 (x^2+1)	000	101	111	010	011	110	100	001
110 (x^2+x)	000	110	001	111	010	100	011	101
111 (x^2+x+1)	000	111	011	100	110	001	101	010

(10) # Number theory

Divisibility

Let $\mathbb{Z}$ denote the set of integers ie $\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$

Defn An integer $a \neq 0$ is said to divide an integer b if $\exists$ an integer k such that $b = ak$. In symbolic form we write a/b ie a divides b

If it is not possible to find an integer k s.t $b = ak$ then we say that a does not divide b ie $a \nmid b$

Congruences

Let m be a positive integer & a, b be any two integers. Then a is said to be congruent to "b modulo m if $a-b$ is divisible by m & is denoted by $a \equiv b \pmod{m}$

Ex:- $13 \equiv 3 \pmod{5}$ ie $5/13-3$ ie $5/10$.

* State & prove Fermat's theorem

Statement:- If p is a prime & $(a, p) = 1$, then $a^{p-1} - 1$ is divisible by p ie $a^{p-1} \equiv 1 \pmod{p}$.

Proof:- To prove $a^{p-1} \equiv 1 \pmod{p}$

ie $a^{p-1} - 1 \equiv 0 \pmod{p}$

$p / a^{p-1} - 1$

using binomial expression

$$(x_1 + x_2)^p = {}^pC_0 x_1^p + {}^pC_1 x_1^{p-1} x_2 + {}^pC_2 x_1^{p-1} x_2^2 + \cdots + {}^pC_{p-1} x_1^1 x_2^{p-1} + {}^pC_p x_2^p$$

$$(x_1 + x_2)^p = (x_1^p + x_2^p) + F(p)$$

where $F(p)$ are the numbers which are divisible by p

(11)

$(x_1+x_2)^p \equiv (x_1^p + x_2^p) \pmod p$

$\therefore (x_1+x_2+\cdots+x_a)^p \equiv (x_1^p + x_2^p + \cdots + x_a^p) \pmod p$

we put $x_1 = x_2 = \cdots = x_a = 1$

we have, $a^p \equiv a \pmod p$

$\because$ gcd of $(a, p) = 1$

$\therefore a^{p-1} \equiv 1 \pmod p$

$\Rightarrow a^{p-1} - 1$ is divisible by p

* State & prove Euler's theorem

Statement: If n is positive & gcd of $(a, n) = 1$ then $a^{\phi(n)} \equiv 1 \pmod n$ where $\phi(n)$ is Euler's of n.

Proof Consider $a_1, a_2 \cdots a_{\phi(n)}$ less than n & relatively prime to n

$\Rightarrow aa_i = aa_j \pmod n$

$a_i a_j \in \{a_1, a_2 \cdots a_{\phi(n)}\}$ $a_i \neq a_j$

$\because$ gcd of $(a, n) = 1 \rightarrow$ given

$\therefore a_i \equiv a_j \pmod n$

$\Rightarrow n \mid a_i - a_j$

$\because a_i \neq a_j$ & also a_i & a_j are less than n & relatively prime to n

$\therefore$ the difference cannot be divided by n.

which is impossible, which is contradiction

$\therefore aa_1, aa_2 \cdots aa_{\phi(n)}$ has different remainder when divided by n

$\Rightarrow aa_1 \equiv a_1' \pmod n$

$\because$ gcd $(a, n) = 1$, gcd $(a_1, n) = 1$

$\Rightarrow$ gcd $(a, a_1, n) = 1$

This shows that $a_1' \in \{a_1, a_2 \cdots a_{\phi(n)}\}$

(12) III[44] $aa_2 \equiv a_2' \pmod n$

$a_2' \in \{a_1, a_2 - a_{\phi(n)}\}$ but $a_1' \neq a_2'$

$\vdots$

$a \cdot a_{\phi(n)} \equiv a'_{\phi(n)} \pmod n$

$\therefore (aa_1)(a \cdot a_2) \cdots (a \cdot a_{\phi(n)}) \equiv a_1' \cdot a_2' \cdots a \cdot a_{\phi(n)} \pmod n$

$\equiv (a_1 \cdot a_2 \cdots a_{\phi(n)}) \bmod n$

$a^{\phi(n)}[a_1 \cdots a_{\phi(n)}] \equiv (a_1 \cdot a_2 \cdots a_{\phi(n)}) \pmod n$

$\gcd(a_1 \cdots a_{\phi(n)}, n) = 1$

$\therefore a^{\phi(n)} \equiv 1 \pmod n$

Euler's funtion $\phi(n)$

let $\phi(n)$ denote the number of positive integers not exceeding n that are relatively prime to n Then the funtion $\phi(n)$ is called as Euler function

Ex:- $\phi(7)$ = No. K. T the no. less than 7 and relatively prime to 7

$= 1, 2, 3, 4, 5, 6.$

$\phi(7) = 6$

$\because \gcd(1,7) = 1$ ✓

" $(2,7) = 1$ ✓

" $(3,7) = 1$ ✓

" $(4,7) = 1$ ✓

" $(5,7) = 1$ ✓

" $(6,7) = 1$ ✓

Now $\phi(8) = 4$

$\because \gcd(1,8) = 1$ ✓

$\gcd(2,8) = X$

$\gcd(3,8) = 1$ ✓

$\gcd(4,8) = X$

$\gcd(5,8) = 1$ ✓

$\gcd(6,8) = X$

$\gcd(7,8) = 1$ ✓

(13) Chinese Remainder Theorem

Procedure to solve

$x \equiv a_1 \pmod{m_1}$

$x \equiv a_2 \pmod{m_2}$

$x \equiv a_3 \pmod{m_3}$

$x \equiv (M_1 x_1 a_1 + M_2 x_2 a_2 + M_3 x_3 a_3) \bmod M$

$M = m_1 \cdot m_2 \cdot m_3$

$M_i = \frac{M}{m_i}$

$M_i x_i \equiv 1 \pmod{m_i}$

Q) Solve using chinese remainder theorem

$x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$, $x \equiv 2 \pmod 7$

$M = m_1 \cdot m_2 \cdot m_3$

$= 3 \cdot 5 \cdot 7 = 105$

$m_1 = 3$, $m_2 = 5$, $m_3 = 7$ check they are relatively prime

$M_1 = \frac{M}{m_1} = \frac{105}{3} = 35$

$M_2 = \frac{M}{m_2} = \frac{105}{5} = 21$

$M_3 = \frac{M}{m_3} = \frac{105}{7} = 15$

$a_1 = 2$, $a_2 = 3$, $a_3 = 2$

$M_i x_i \equiv 1 \pmod{m_i}$

$M_1 x_1 \equiv 1 \pmod{m_1}$

$35 x_1 \equiv 1 \pmod 3$

$35 x_1 \pmod 3 \equiv 1$

$[2 x_1 \equiv 1 \pmod 3] \times 2$

$4 x_1 \equiv 2 \pmod 3$

$1 x_1 \equiv 2 \bmod 5$

$\boxed{x_1 = 2}$

$3 \overline{)35}$ (11), 33, 2

3 → 4
6 → 7
9 → 10
12 → 13

$M_2 x_2 \equiv 1 \pmod{m_2}$

$21 x_2 \equiv 1 \pmod 5$

$1 x_2 \equiv 1 \pmod 5$

$\boxed{x_2 \equiv 1}$

5) 21 (4
20
1

$M_3 x_3 \equiv 1 \pmod{m_3}$

$15 x_3 \equiv 1 \pmod 7$

$1 x_3 \equiv 1 \pmod 7$.

$\boxed{x_3 = 1}$

7) 15 (2
14
1

Now

$x \equiv (M_1 x_1 a_1 + M_2 x_2 a_2 + M_3 x_3 a_3) \pmod M$

$\equiv (35 \times 2 \times 2 + 21 \times 1 \times 3 + 15 \times 2 \times 1) \pmod{105}$

$\equiv 176 \pmod{105}$

or $x \equiv 71 \pmod{105}$

105) 176 (1
105
71

Verification

$176 - 105 = 71 - 105 = -34$

$x = 34 \Rightarrow$ ~~34 mod 3 = 1~~

~~84 mod 5 = 4~~

~~34 mod 7 =~~

2) $x \equiv 1 \pmod 5$, $x \equiv 1 \pmod 7$ $x \equiv 3 \pmod{11}$

$M = m_1 m_2 m_3$

$M = 5 \times 7 \times 11 = 385$

$m_1 = 5$
$m_2 = 7$
$m_3 = 11$
} relatively prime

$a_1 = 1$, $a_2 = 1$, $a_3 = 3$

$M_i = \frac{M}{m_i}$

$M_1 = \frac{M}{m_1} = \frac{385}{5} = 77$

$M_2 = \frac{M}{m_2} = \frac{385}{7} = 55$

$M_3 = \frac{M}{m_3} = \frac{385}{11} = 35$

$M_i x_i \equiv 1 \pmod{m_i}$

$M_1 x_1 \equiv 1 \pmod 5$

$77 x_1 \equiv 1 \pmod 5$

~~$2x_1 \equiv 1 \pmod 5$~~

$77 x_1 \pmod 5 \equiv 1$

$2x_1 \equiv 1 \pmod 5$ $\times 3$ → Refer the reasoning given below

$6x_1 \equiv 3 \pmod 5$

$1x_1 \equiv 3 \pmod 5$

$\boxed{x_1 = 3}$

$M_2 x_2 \equiv 1 \pmod{m_2}$

$55 x_2 \equiv 1 \pmod 7$

$6x_2 \equiv 1 \pmod 7$

$6x_2 \equiv 1 \pmod 7$ $\times 6$ → reason it is multiplied by 6 because remainder will be 1 ie $7\overline{)36}\,(5$, $\frac{35}{1}$

$36x_2 \equiv 6 \pmod 7$

$1x_2 \equiv 6 \pmod 7$

$\boxed{x_2 = 6}$

$7\overline{)55}\,(7$, $\frac{49}{6}$

7 → 8, 14 → 15, 21 → 22, 28 → 29, (35 → 36)

$M_3 x_3 \equiv 1 \pmod{m_3}$

$35 x_3 \equiv 1 \pmod{11}$

$2x_3 \equiv 1 \pmod{11}$ $\times 6$

$12x_3 \equiv 1 \pmod{11}$

$1x_3 \equiv 1 \pmod{11}$

$\boxed{x_3 = 1}$

$11\overline{)35}\,(3$, $\frac{33}{2}$

$x = (M_1 x_1 a_1 + M_2 x_2 a_2 + M_3 x_3 a_3) \pmod M$

$x = (77 \times 3 \times 1 + 55 \times 6 \times 1 + 35 \times 1 \times 3) \pmod{385}$

$x \equiv 1191 \pmod{385}$ //

1 SYMMETRIC CIPHER MODEL

A symmetric encryption scheme has five ingredients (Figure 1):

- ***Plaintext:*** This is the original intelligible message or data that is fed into the algorithm as input.

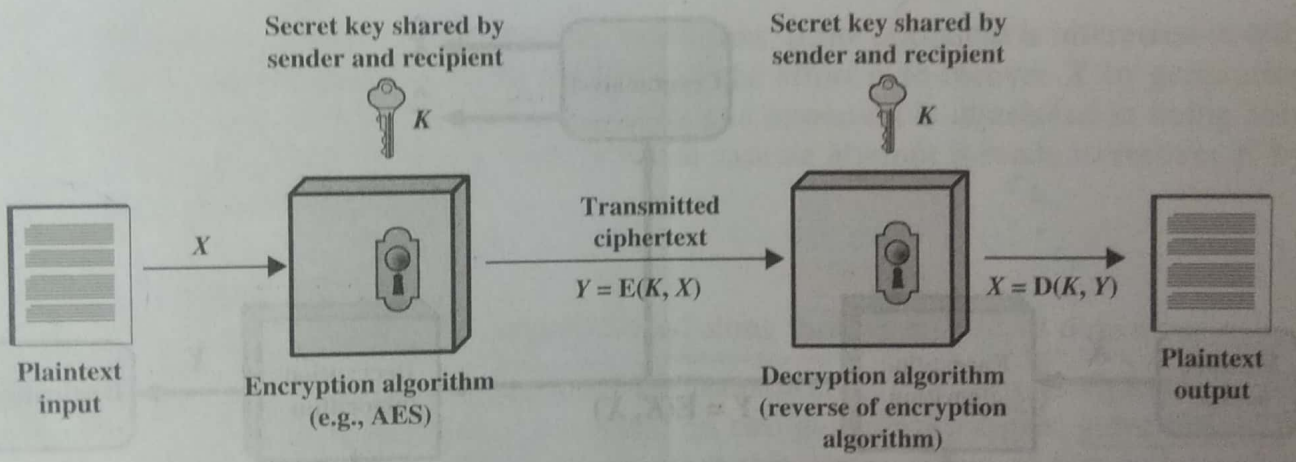

Figure 1 Simplified Model of Symmetric Encryption

- **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.

Cryptography

Cryptographic systems are characterized along three independent dimensions:

1. **The type of operations used for transforming plaintext to ciphertext.** All encryption algorithms are based on two general principles: substitution, in which each element in the plaintext (bit, letter, group of bits or letters) is mapped into another element, and transposition, in which elements in the plaintext are rearranged. The fundamental requirement is that no information be lost (i.e., that all operations are reversible). Most systems, referred to as *product systems*, involve multiple stages of substitutions and transpositions.
2. **The number of keys used.** If both sender and receiver use the same key, the system is referred to as symmetric, single-key, ~~secret-key, or conventional encryption~~. If the sender and receiver use different keys, the system is referred to as asymmetric, two-key, ~~or public-key encryption~~.
3. **The way in which the plaintext is processed.** A *block cipher* processes the input one block of elements at a time, producing an output block for each input block. A *stream cipher* processes the input elements continuously, producing output one element at a time, as it goes along.

Caesar Cipher

The earliest known, and the simplest, use of a substitution cipher was by Julius Caesar. The Caesar cipher involves replacing each letter of the alphabet with the letter standing three places further down the alphabet. For example,

```
plain:  meet me after the toga party
cipher: PHHW PH DIWHU WKH WRJD SDUWB
```

Note that the alphabet is wrapped around, so that the letter following Z is A. We can define the transformation by listing all possibilities, as follows:

```
plain:  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
cipher: 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
```

Let us assign a numerical equivalent to each letter:

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12

n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

Then the algorithm can be expressed as follows. For each plaintext letter p, substitute the ciphertext letter C:[2]

$$C = \mathrm{E}(3, p) = (p + 3) \bmod 26$$

A shift may be of any amount, so that the general Caesar algorithm is

$$C = \mathrm{E}(k, p) = (p + k) \bmod 26 \quad (1)$$

where k takes on a value in the range 1 to 25. The decryption algorithm is simply

$$p = \mathrm{D}(k, C) = (C - k) \bmod 26 \quad (2)$$

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. Figure 3 shows the results of applying this strategy to the example ciphertext. In this case, the plaintext leaps out as occupying the third line.

Three important characteristics of this problem 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.

TESTING FOR PRIMALITY

For many cryptographic algorithms, it is necessary to select one or more very large prime numbers at random. Thus, we are faced with the task of determining whether a given large number is prime. There is no simple yet efficient means of accomplishing this task.

In this section, we present one attractive and popular algorithm. You may be surprised to learn that this algorithm yields a number that is not necessarily a prime. However, the algorithm can yield a number that is almost certainly a prime. This will be explained presently. We also make reference to a deterministic algorithm for finding primes. The section closes with a discussion concerning the distribution of primes.

Miller-Rabin Algorithm[7]

The algorithm due to Miller and Rabin [MILL75, RABI80] is typically used to test a large number for primality. Before explaining the algorithm, we need some background. First, any positive odd integer $n \geq 3$ can be expressed as

$$n - 1 = 2^k q \qquad \text{with } k > 0, q \text{ odd}$$

To see this, note that $n - 1$ is an even integer. Then, divide $(n - 1)$ by 2 until the result is an odd number q, for a total of k divisions. If n is expressed as a binary number, then the result is achieved by shifting the number to the right until the

Algorithm on Testing of primality

~~MORE NUMBER THEORY~~

```
TEST (n)
1. Find integers k, q, with k > 0, q odd, so that
   (n − 1 = 2^k q);
2. Select a random integer a, 1 < a < n − 1;
3. if a^q mod n = 1 then return("inconclusive");
4. for j = 0 to k − 1 do
5. if a^(2^j q) mod n = n − 1 then return("inconclusive");
6. return("composite");
```

Public-Key Cryptosystems

Asymmetric algorithms rely on one key for encryption and a different but related key for decryption. These algorithms have the following important characteristic.

- It is computationally infeasible to determine the decryption key given only knowledge of the cryptographic algorithm and the encryption key.

- **Encryption algorithm:** The encryption algorithm performs various transformations on the plaintext.
- **Public and private keys:** This is a pair of keys that have been selected so that if one is used for encryption, the other is used for decryption. The exact transformations performed by the algorithm depend on the public or private key that is provided as input.
- **Ciphertext:** This is the scrambled message produced as output. It depends on the plaintext and the key. For a given message, two different keys will produce two different ciphertexts.
- **Decryption algorithm:** This algorithm accepts the ciphertext and the matching key and produces the original plaintext.

The essential steps are the following.

1. Each user generates a pair of keys to be used for the encryption and decryption of messages.
2. Each user places one of the two keys in a public register or other accessible file. This is the public key. The companion key is kept private. As Figure 1a suggests, each user maintains a collection of public keys obtained from others.
3. If Bob wishes to send a confidential message to Alice, Bob encrypts the message using Alice's public key.
4. When Alice receives the message, she decrypts it using her private key. No other recipient can decrypt the message because only Alice knows Alice's private key.

With this approach, all participants have access to public keys, and private keys are generated locally by each participant and therefore need never be distributed. As long as a user's private key remains protected and secret, incoming communication is secure. At any time, a system can change its private key and publish the companion public key to replace its old public key.

Table 2 summarizes some of the important aspects of symmetric and public-key encryption. To discriminate between the two, we refer to the key used in symmetric encryption as a **secret key**. The two keys used for asymmetric encryption are referred to as the **public key** and the **private key**.[2] Invariably, the private key is kept secret, but it is referred to as a private key rather than a secret key to avoid confusion with symmetric encryption.

Let us take a closer look at the essential elements of a public-key encryption scheme, using Figure 2. There is some source A that produces a message in plaintext, $X = [X_1, X_2, \ldots, X_M]$. The M elements of X are letters in some finite alphabet. The message is intended for destination B. B generates

Description of the Algorithm

RSA makes use of an expression with exponentials. Plaintext is encrypted in blocks, with each block having a binary value less than some number n. That is, the block size must be less than or equal to $\log_2(n) + 1$; in practice, the block size is i bits, where $2^i < n \leq 2^{i+1}$. Encryption and decryption are of the following form, for some plaintext block M and ciphertext block C.

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

$$M = C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n$$

Both sender and receiver must know the value of n. The sender knows the value of e, and only the receiver knows the value of d. Thus, this is a public-key encryption algorithm with a public key of $PU = \{e, n\}$ and a private key of $PR = \{d, n\}$. For this algorithm to be satisfactory for public-key encryption, the following requirements must be met.

1. It is possible to find values of e, d, and n such that $M^{ed} \bmod n = M$ for all $M < n$.
2. It is relatively easy to calculate $M^e \bmod n$ and $C^d \bmod n$ for all values of $M < n$.
3. It is infeasible to determine d given e and n.

For now, we focus on the first requirement and consider the other questions later. We need to find a relationship of the form

$$M^{ed} \bmod n = M$$

The preceding relationship holds if e and d are multiplicative inverses modulo $\phi(n)$, where $\phi(n)$ is the Euler totient function. For p, q prime, $\phi(pq) = (p - 1)(q - 1)$. The relationship between e and d can be expressed as

$$ed \bmod \phi(n) = 1 \tag{1}$$

This is equivalent to saying

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

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

That is, e and d are multiplicative inverses mod $\phi(n)$. Note that, according to the rules of modular arithmetic, this is true only if d (and therefore e) is relatively prime to $\phi(n)$. Equivalently, $\gcd(\phi(n), d) = 1$. Equation (1) satisfies the requirement for RSA.

Cryptography

RSA algorithm

Public Key Cryptography

- 1 Key → private Key (Encryption/decryption)
- 2 Keys → private Key (Encryption)
  → Public Key (decryption)

RSA algorithm

(Rivest Shamir Adleman) algorithm

1) Choose two different prime numbers p, q
2) Calculate modulus $n = p \times q$
3) Calculate totient function
   $\phi(x) = (p-1)(q-1)$
4) Choose an integer e s.t $1 < e < \phi(n)$ & $\gcd(e, \phi(n)) = 1$ where e is public key
5) Calculate $d = \frac{1 + K\phi(n)}{e}$ $\because ed \equiv 1 \bmod \phi(n)$ (using extended Euclidean algorithm)

Encryption

$C = M^e \bmod n$ (where M is the message given)

Decryption

$M = C^d \bmod n$ (where C → Ciphertext)

Ex 1) Perform encryption & decryption using the RSA algorithm for $p=3, q=5, M=2$.

1) $p=3, q=5$

2) $n = pq = 3 \times 5 = 15$

3) $\phi(n) = (p-1)(q-1) = 2 \times 4 = 8$

4) $e = 7$ $\because 1 < 7 < 8$ & $\gcd(7,8)=1$.
$1 < e < \phi(n)$

5) $d = \frac{1 + k\phi(n)}{e}$ $k = 0, 1, 2, 3, 4, 5, 6$ $k < e$

Let $k=6$ (take such a value of k s.t d is an integer value)

$$d = \frac{1+6\times 8}{7} = \frac{49}{7} = 7$$

Encryption $M=2$ $C = M^e \bmod n$

$C = 2^7 \bmod 15 = 128 \bmod 15 = 8$

Decryption

$M = C^d \bmod n$

$= 8^7 \bmod 15$

$= 2097152 \bmod 15$

$M = 2$

2) Perform encryption & decryption using the RSA algorithm for $p=5, q=11, e=3, M=9$

1) $p = 5$, $q = 11$

2) $n = pq = 5 \times 11 = 55$

3) $\phi(n) = (p-1)(q-1) = 4 \times 10 = 40$

4) $e = 3$, $1 < 3 < 40$ & $\gcd(3, 40) = 1$

5) $d = \frac{1 + K\phi(n)}{e}$ $K = 0, 1, 2$

$K = 2$

$= \frac{1 + 2 \times 40}{3} = \frac{81}{3} = 27$

Encryption $M = 9$

$C = M^e \bmod n$

$C = 9^3 \bmod 55 = 729 \bmod 55$

$= 14$

$M = C^d \bmod n$

$= 14^{27} \bmod 55$

$14^{27} \bmod 55 = (14^1 \bmod 55) \times (14^2 \bmod 55) \times (14^4 \bmod 55)$

$\times (14^4 \bmod 55) \times (14^8 \bmod 55) \times (14^8 \bmod 55) \bmod 55$

$14^1 \bmod 55 = 14$

$14^2 \bmod 55 = 196 \bmod 55 = 31$

$14^4 \bmod 55 = 38416 \bmod 55 = 26$

$14^8 \bmod 55 = 1475789056 \bmod 55 = 16$

$= (14 \times 31 \times 26 \times 26 \times 16 \times 16) \bmod 55$

$= 75106304 \bmod 55$

$= 9$

$\therefore M = 14^{27} \bmod 55 = 9.$