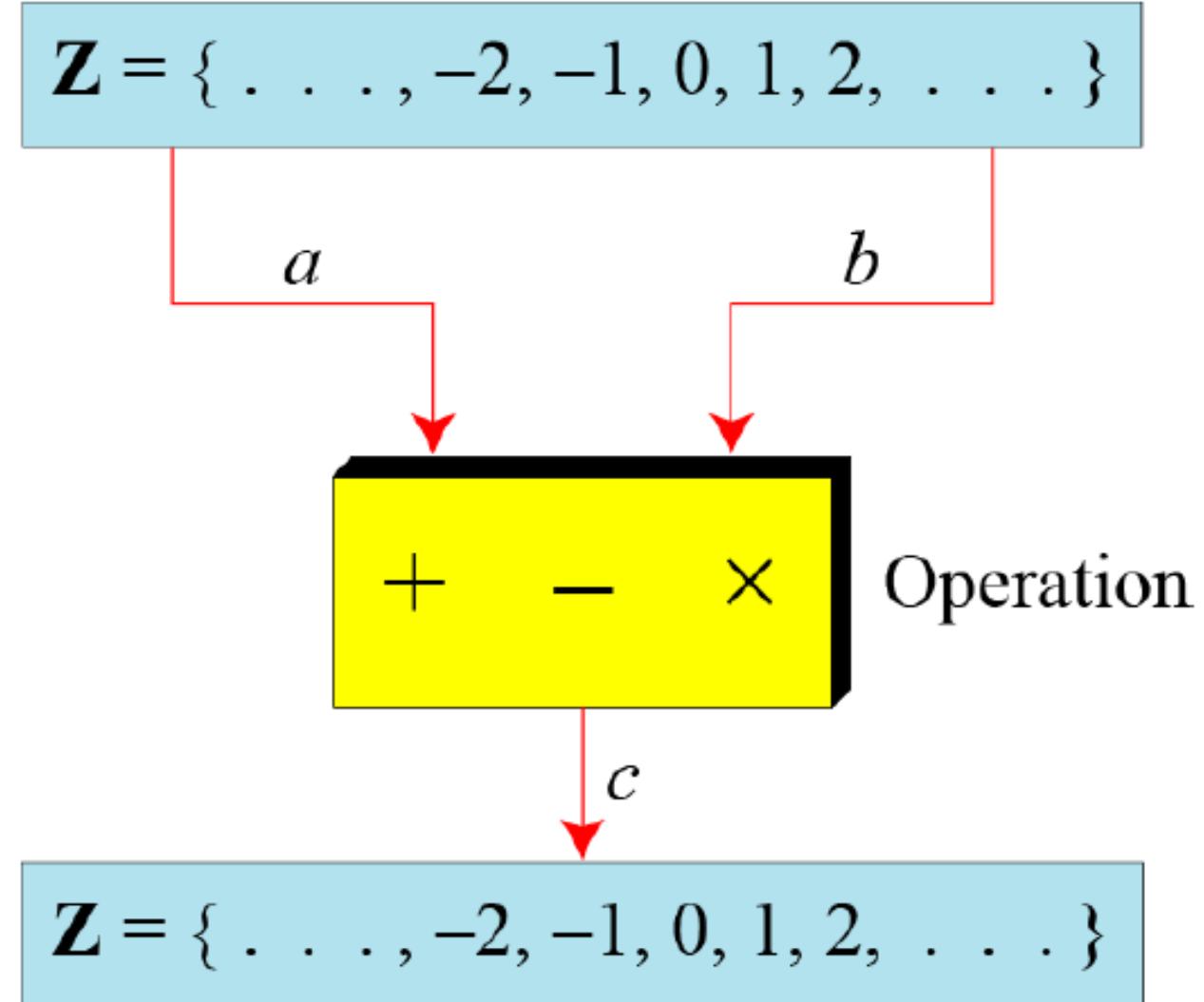


Integer Arithmetic

- Consists of a set of Integers and operations on it.



Integer Division

- If $b|a$ and $b \neq 0$, then $a = q * b$; where $a, b, q \in \mathbb{Z}$
- If $b \nmid a$ and $b \neq 0$, then $a = q * b + r$; where $a, b, q, r \in \mathbb{Z}$

$$-255 = (-23 \times 11) + (-2) \quad \leftrightarrow \quad -255 = (-24 \times 11) + 9$$

Properties of Integer Division

- If $b|a$ and $a|b$, then $a=\pm b$.
- If $b|1$, then $b=\pm 1$.
- If $a|b$ and $b|c$, then $a|c$.
- If $a|b$ and $a|c$, then $a|(m*b+n*c)$, where $a, b, c, m, n \in \mathbb{Z}$.

MODULAR ARITHMETIC

Modular Arithmetic

- For $a = q * b + r$,
- $a \bmod b = r$; where $a, b, q, r \in \mathbb{Z}$.
- $\mathbb{Z}_n = \{0, 1, 2, 3, 4, \dots, (n - 1)\}$

$$\mathbb{Z}_2 = \{0, 1\}$$

$$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$$

$$\mathbb{Z}_{11} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$$

Modular Arithmetic (Examples)

- $27 \bmod 5 = 2$
- $36 \bmod 7 = 1$
- $-13 \bmod 6 = 5$
- $-29 \bmod 12 = 7$



Basic Operations in Modular Arithmetic

- 
- If $a, b \in Z_n$, then $(a + b) \bmod n = c \in Z_n$
 - If $a, b \in Z_n$, then $(a - b) \bmod n = c \in Z_n$
 - If $a, b \in Z_n$ then $(a * b) \bmod n = c \in Z_n$

Basic Operations in Modular Arithmetic (Examples)

- $(17 + 19) \bmod 23 = 13 \in Z_{23}$
- $(3 - 5) \bmod 6 = 4 \in Z_6$
- $(13 * 14) \bmod 15 = 2 \in Z_{15}$
- $(8 * 9) \bmod 13 = 7 \in Z_{13}$

Properties of Modular Arithmetic

$$(a + b) \bmod n = [(a \bmod n) + (b \bmod n)] \bmod n; a, b \in \mathbb{Z}$$
$$(a - b) \bmod n = [(a \bmod n) - (b \bmod n)] \bmod n; a, b \in \mathbb{Z}$$
$$(a * b) \bmod n = [(a \bmod n) * (b \bmod n)] \bmod n; a, b \in \mathbb{Z}$$

Properties of Modular Arithmetic (Examples)

$$(8 + 7) \bmod 5 = [(8 \bmod 5) + (7 \bmod 5)] \bmod 5 = (3 + 2) \bmod 5 = 0 \in Z_5$$

$$(28 - 16) \bmod 8 = [(28 \bmod 8) - (16 \bmod 8)] \bmod 8 = (4 - 0) \bmod 8 = 4 \in Z_8$$

$$(23 * 25) \bmod 20 = [(23 \bmod 20) * (25 \bmod 20)] \bmod 20 = (3 * 5) \bmod 20 = 15 \in Z_{20}$$

Modular Additive Inverse

For $a, b \in Z_n$, b is the additive inverse of a if $(a + b) \equiv 0 \pmod{n}$

Additive Inverse pairs of $Z_{10} = \{(0,0), (1,9), (2,8), (3,7), (4,6), (5,5)\}$

Additive Inverse pairs of $Z_9 = \{(0,0), (1,8), (2,7), (3,6), (4,5)\}$

Additive Inverse pairs of $Z_{11} = \{(0,0), (1,10), (2,9), (3,8), (4,7), (5,6)\}$

Modular Multiplicative Inverse

*For $a, b \in Z_n$, b is the Multiplicative Inverse of a , if $(a * b) \equiv 1 \pmod{n}$*

Multiplicative Inverse pairs in $Z_5 = \{(1,1), (2,3), (4,4)\}$

Multiplicative Inverse pairs in $Z_6 = \{(1,1), (5,5)\}$

Multiplicative Inverse pairs in $Z_7 = \{(1,1), (2,4), (3,5), (6,6)\}$

Properties of Congruences

- 1) Reflexive Property:- $a \equiv a \pmod{n}$
- 2) Symmetric Property:- *If $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$*
- 3) Transitive Property:- *If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$*
- 4) Addition Property:- *If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $(a + c) \equiv (b + d) \pmod{n}$*
- 5) Subtraction Property:- *If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $(a - c) \equiv (b - d) \pmod{n}$*
- 6) Multiplication Property:- *If $a \equiv b \pmod{n}$, then $(a * c) \equiv (b * c) \pmod{n}$; $c \in \mathbb{Z}$*
- 7) Exponential Property:- *If $a \equiv b \pmod{n}$, then $a^m \equiv b^m \pmod{n}$*

Properties of Congruences (Examples)

- $7 \equiv 7 \pmod{5}$
- $8 \equiv 3 \pmod{5}$; Hence, $3 \equiv 8 \pmod{5}$
- $18 \equiv 11 \pmod{7}$; $11 \equiv 4 \pmod{7}$; Hence, $18 \equiv 4 \pmod{7}$
- $19 \equiv 10 \pmod{9}$; $25 \equiv 16 \pmod{9}$; Hence, $44 \equiv 26 \pmod{9}$
- $44 \equiv 26 \pmod{9}$; $25 \equiv 16 \pmod{9}$; Hence, $19 \equiv 10 \pmod{9}$
- $18 \equiv 11 \pmod{7}$; Hence, $90 \equiv 55 \pmod{7}$
- $8 \equiv 3 \pmod{5}$; Hence, $64 \equiv 9 \pmod{5}$;

PRIMES AND GCD

Prime Numbers

- In Cryptography, only positive primes have significance, though some Mathematicians extend the idea of primes and composites to negative numbers as well.
- In Cryptography, large primes are required for algorithms like RSA, Diffie Hellman, etc.

2039568783564019774057658669290345772801939933143482630947726464532830627
2270127763293661606314408817331237288267712387953870940015830656733832827
9154499698366071906766440037074217117805690872792848149112022286332144876
1833763265120835748216479339929612499173198362193042742802438031040150005
63790123

Prime Factorization

- Expressing a positive composite number as a product of primes.
- Prime factorization of a number is harder than multiplying the primes to generate the number.
- $10 = 2 * 5$
- $100 = 2^2 * 5^2$
- $1000 = 2^3 * 5^3$
- $120 = 2^3 * 3 * 5$
- $5040 = 2^4 * 3^2 * 5 * 7$

GCD (HCF)



- In Cryptography, typically only positive numbers are used.
- *If $c|a$ and $c|b$, then $\text{GCD}(a, b) = c$; where $a, b, c \in N$.*
- $\text{GCD}(5, 10) = 5$
- $\text{GCD}(8, 12) = 4$
- $\text{GCD}(24, 60) = 12$
- $\text{GCD}(10, 45) = 5$
- $\text{GCD}(28, 70) = 14$

Co-Primes



- a and b are co-prime if $\text{GCD}(a,b) = 1$; $a,b \in \mathbb{N}$;
- 1 is co-prime with all the Natural numbers.
- For $a \equiv b \pmod{n}$, if $\text{GCD}(d,n)=1$, then $(a/d) \equiv (b/d) \pmod{n}$; where $d \in \mathbb{N}$.
- Examples of some co-prime pairs: (8,15), (12,25), (17,20)

EUCLIDEAN ALGORITHM

Euclidean Algorithm to Calculate GCD (Pseudocode)

```
GCD(a,b)
{
    if(b==0)
        return a;
    else
        return GCD(b, a mod b)
}
```



- Here $a, b \in \mathbb{N}$ and $a \geq b$.

$\text{GCD}(48, 18) = ?$

a	b
48	18
18	12
12	6
6	0

$\text{GCD}(198, 121) = ?$

a	b
198	121
121	77
77	44
44	33
33	11
11	0

GCD (584, 248) = ?

a	b
584	248
248	88
88	72
72	16
16	8
8	0

GCD (66348, 18042) = ?

a	b
66348	18042
18042	12222
12222	5820
5820	582
582	0

GCD (868, 795) = ?

a	b
868	795
795	73
73	65
65	8
8	1
1	0

EXTENDED EUCLIDEAN ALGORITHM (EEA)

EEA for $\text{gcd}(a,b)=d$

```
EEA(a, b)
{
    u1=1, u2=0, v1=0, v2=1;
    while(b≠0)
    {
        q=a/b; r=a mod b; u=u1-q*u2; v=v1-q*v2;
        a=b; b=r; u1=u2; u2=u; v1=v2; v2=v;
    }
    d=a; x=u1; y=v1;
    return(d, x, y)
}
```

- Here $d=a*x+b*y$; where $x,y \in \mathbb{Z}$.

Calculate GCD(48,18), x, y

q	a	b	r	u1	u2	u	v1	v2	v
2	48	18	12	1	0	1	0	1	-2
1	18	12	6	0	1	-1	1	-2	3
2	12	6	0	1	-1	3	-2	3	-8
	6	0		-1	3		3	-8	

- $\text{GCD}(48, 18) = 6 = 48 * (-1) + 18 * (3)$

Calculate GCD(848, 596), x, y

q	a	b	r	u1	u2	u	v1	v2	v
1	848	596	252	1	0	1	0	1	-1
2	596	252	92	0	1	-2	1	-1	3
2	252	92	68	1	-2	5	-1	3	-7
1	92	68	24	-2	5	-7	3	-7	10
2	68	24	20	5	-7	19	-7	10	-27
1	24	20	4	-7	19	-26	10	-27	37
5	20	4	0	19	-26	149	-27	37	-212
	4	0		-26	149		37	-212	

- $\text{GCD}(848, 596) = 4 = 848 * (-26) + 596 * (37)$

Calculate GCD(165,68), x, y

q	a	b	r	u1	u2	u	v1	v2	v
2	165	68	29	1	0	1	0	1	-2
2	68	29	10	0	1	-2	1	-2	5
2	29	10	9	1	-2	5	-2	5	-12
1	10	9	1	-2	5	-7	5	-12	17
9	9	1	0	5	-7	68	-12	17	-165
	1	0		-7	68		17	-165	

- $\text{GCD}(165,68) = 1 = 165*(-7)+68*(17)$
- Hence, $\text{MI}(165) \bmod 68 = -7 \bmod 68 = 61$

MI(485) mod 812 = ?

q	a	b	r	v1	v2	v
1	812	485	327	0	1	-1
1	485	327	158	1	-1	2
2	327	158	11	-1	2	-5
14	158	11	4	2	-5	72
2	11	4	3	-5	72	-149
1	4	3	1	72	-149	221
3	3	1	0	-149	221	-812
	1	0		221	-812	

- $\text{MI}(485) \bmod 812 = 221$

$\text{MI}(608) \bmod 73 = ?$

q	a	b	r	u1	u2	u
8	608	73	24	1	0	1
3	73	24	1	0	1	-3
24	24	1	0	1	-3	73
	1	0		-3	73	

- $\text{MI}(608) \bmod 73 = -3 \bmod 73 = 70$

MODULAR EXPONENTIAL ALGORITHM

$$7^{13} \bmod 20 = ?$$

- $7^4 \bmod 20 = 1$
- $7^{13} \bmod 20 = [7^{12} \bmod 20 * 7 \bmod 20] \bmod 20$
- $7^{13} \bmod 20 = (7^4 \bmod 20)^3 \bmod 20 * 7 \bmod 20 = 7$

$$13^{27} \bmod 48 = ?$$

- $27 = 16+8+2+1$
- $13^2 \bmod 48 = 25$
- $13^8 \bmod 48 = (13^2 \bmod 48)^4 \bmod 48 = 25^4 \bmod 48 = 1$
- $13^{16} \bmod 48 = (13^8 \bmod 48)^2 \bmod 48 = 1^2 \bmod 48 = 1$
- $13^{27} \bmod 48 = (13^{16} \bmod 48 * 13^8 \bmod 48 * 13^2 \bmod 48 * 13) \bmod 48 = (1 * 1 * 25 * 13) \bmod 48 = 37$

$$106^{239} \bmod 54 = ?$$

-
- $239 = 128 + 64 + 32 + 8 + 4 + 2 + 1$
 - $106^2 \bmod 54 = 4$
 - $106^4 \bmod 54 = (106^2 \bmod 54)^2 \bmod 54 = 4^2 \bmod 54 = 16$
 - $106^8 \bmod 54 = (106^4 \bmod 54)^2 \bmod 54 = 16^2 \bmod 54 = 40$
 - $106^{32} \bmod 54 = (106^8 \bmod 54)^4 \bmod 54 = 40^4 \bmod 54 = 22$
 - $106^{64} \bmod 54 = (106^{32} \bmod 54)^2 \bmod 54 = 22^2 \bmod 54 = 52$
 - $106^{128} \bmod 54 = (106^{64} \bmod 54)^2 \bmod 54 = 52^2 \bmod 54 = 4$
 - $106^{239} \bmod 54 = (106^{128} \bmod 54 * 106^{64} \bmod 54 * 106^{32} \bmod 54 * 106^8 \bmod 54 * 106^4 \bmod 54 * 106^2 \bmod 54 * 106) \bmod 54$

$$106^{239} \bmod 54 = ? \text{ (Contd..)}$$

-
- $106^{239} \bmod 54 = (4*52*22*40*16*4*106) \bmod 54$
 - $106^{239} \bmod 54 = [(4*52*22*40) \bmod 54 * (16*4*106) \bmod 54] \bmod 54$
 - $106^{239} \bmod 54 = (34 * 34) \bmod 54 = 22$

FERMAT'S THEOREM

Fermat's Theorem

- $a^{p-1} \equiv 1 \pmod{p}$; where $a \in \mathbb{N}$, $\text{GCD}(a,p)=1$, and p is a prime.
- $7^{18} \pmod{19} = 1$
- $48^{28} \pmod{29} = 1$
- $65^{96} \pmod{97} = 1$

Fermat's Theorem (Proof)

Consider the set of positive integers less than p : $\{1, 2, \dots, p - 1\}$ and multiply each element by a , modulo p , to get the set $X = \{a \bmod p, 2a \bmod p, \dots, (p - 1)a \bmod p\}$. None of the elements of X is equal to zero because p does not divide a . Furthermore, no two of the integers in X are equal. To see this, assume that $ja \equiv ka \pmod{p}$, where $1 \leq j < k \leq p - 1$. Because a is relatively prime to p , we can eliminate a from both sides of the equation resulting in $j \equiv k \pmod{p}$. This last equality is impossible, because j and k are both positive integers less than p . Therefore, we know that the $(p - 1)$ elements of X are all positive integers with no two elements equal. We can conclude the X consists of the set of integers $\{1, 2, \dots, p - 1\}$ in some order. Multiplying the numbers in both sets (p and X) and taking the result mod p yields

$$\begin{aligned} a \times 2a \times \dots \times (p - 1)a &\equiv [(1 \times 2 \times \dots \times (p - 1)] \pmod{p} \\ a^{p-1}(p - 1)! &\equiv (p - 1)! \pmod{p} \end{aligned}$$

Fermat's Theorem (Proof)

- Dividing both the sides of the equation by $(p-1)!$ (Since its coprime with p), we get $a^{p-1} \equiv 1 \pmod{p}$, which represents the Fermat's theorem
- If we multiply both the sides of the equation representing the Fermat's theorem by a , then we also get $a^p \equiv a \pmod{p}$

Fermat's Theorem (Examples)

- $7^{19} \bmod 19 = 7$
- $48^{29} \bmod 29 = 48 \bmod 29 = 19$
- $140^{73} \bmod 73 = 140 \bmod 73 = 67$

$$200^{192} \bmod 97 = ?$$

- $200^{96} \bmod 97 = 1$
- $200^{192} \bmod 97 = (200^{96} \bmod 97)^2 \bmod 97 = 1^2 \bmod 97 = 1$

$$3^{1026} \bmod 103 = ?$$

- $3^{102} \bmod 103 = 1$
- $3^{1020} \bmod 103 = (3^{102} \bmod 103)^{10} \bmod 103 = 1^{10} \bmod 13 = 1$
- $3^{1026} \bmod 103 = (3^{1020} \bmod 103 * 3^6 \bmod 103) \bmod 103$
- $3^{1026} \bmod 103 = (1 * 8) \bmod 103 = 8$

EULER'S THEOREM

Euler Totient Function ($\phi(n)$)

- $\phi(n)$ = Number of natural numbers less than n which are relatively prime with n.
- $\phi(p) = p-1$; p is a prime.
- If $n = p^m q^n$, then $\phi(n) = (p-1)^m (q-1)^n$, where p and q are primes and $p \neq q$
- If $n=p^m$, $\phi(n) = p^m - p^{m-1}$

Proof for $\phi(n) = \phi(p * q) = \phi(p) * \phi(q)$

To see that $\phi(n) = \phi(p) \times \phi(q)$, consider that the set of positive integers less than n is the set $\{1, \dots, (pq - 1)\}$. The integers in this set that are not relatively prime to n are the set $\{p, 2p, \dots, (q - 1)p\}$ and the set $\{q, 2q, \dots, (p - 1)q\}$. To see this, consider that any integer that divides n must divide either of the prime numbers p or q . Therefore, any integer that does not contain either p or q as a factor is relatively prime to n . Further note that the two sets just listed are non-overlapping:

Proof for $\phi(n) = \phi(p^*q) = \phi(p)*\phi(q)$ (Contd..)

Because p and q are prime, we can state that none of the integers in the first set can be written as a multiple of q , and none of the integers in the second set can be written as a multiple of p . Thus the total number of unique integers in the two sets is $(q - 1) + (p - 1)$. Accordingly,

$$\begin{aligned}\phi(n) &= (pq - 1) - [(q - 1) + (p - 1)] \\&= pq - (p + q) + 1 \\&= (p - 1) \times (q - 1) \\&= \phi(p) \times \phi(q)\end{aligned}$$

Euler's Theorem

If $\text{GCD}(a,n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod{n}$

Euler's Theorem (Proof)

Equation \dots is true if n is prime, because in that case, $\phi(n) = (n - 1)$ and Fermat's theorem holds. However, it also holds for any integer n . Recall that $\phi(n)$ is the number of positive integers less than n that are relatively prime to n . Consider the set of such integers, labeled as

$$R = \{x_1, x_2, \dots, x_{\phi(n)}\}$$

That is, each element x_i of R is a unique positive integer less than n with $\gcd(x_i, n) = 1$. Now multiply each element by a , modulo n :

$$S = \{(ax_1 \bmod n), (ax_2 \bmod n), \dots, (ax_{\phi(n)} \bmod n)\}$$

The set S is a permutation of R , by the following line of reasoning:

1. Because a is relatively prime to n and x_i is relatively prime to n , ax_i must also be relatively prime to n . Thus, all the members of S are integers that are less than n and that are relatively prime to n .

Euler's Theorem (Proof)

2. There are no duplicates in S .
 $= ax_j \bmod n$, then $x_i = x_j$.

If $ax_i \bmod n$

Therefore,

$$\begin{aligned} \prod_{i=1}^{\phi(n)} (ax_i \bmod n) &= \prod_{i=1}^{\phi(n)} x_i \\ \prod_{i=1}^{\phi(n)} ax_i &\equiv \prod_{i=1}^{\phi(n)} x_i \pmod{n} \\ a^{\phi(n)} \times \left[\prod_{i=1}^{\phi(n)} x_i \right] &\equiv \prod_{i=1}^{\phi(n)} x_i \pmod{n} \\ a^{\phi(n)} &\equiv 1 \pmod{n} \end{aligned}$$

$33^{40} \bmod 100 = ?$

- $\text{GCD}(33,100) = 1$
- $\phi(100) = \phi(2^2) * \phi(5^2) = (2^2 - 2) * (5^2 - 5) = 40$
- Hence $33^{40} \bmod 100 = 1$

$77^{1218} \text{ mod } 240 = ?$

- $\text{GCD}(77, 240)=1$
- $\phi(240) = \phi(2^4) * \phi(3) * \phi(5) = 8*2*4 = 64$
- $77^{64} \text{ mod } 240 = 1$
- $77^{1218} \text{ mod } 240 = [(77^{64} \text{ mod } 240)^{19} * 77^2 \text{ mod } 240] \text{ mod } 240$
- $77^{1218} \text{ mod } 240 = (1*169) \text{ mod } 240 = 169$

PRIMALITY TESTING

Primality Testing (Properties)

The **first property** is stated as follows: If p is prime and a is a positive integer less than p , then $a^2 \bmod p = 1$ if and only if either $a \bmod p = 1$ or $a \bmod p = -1 \bmod p = p - 1$. By the rules of modular arithmetic $(a \bmod p)(a \bmod p) = a^2 \bmod p$. Thus, if either $a \bmod p = 1$ or $a \bmod p = -1$, then $a^2 \bmod p = 1$. Conversely, if $a^2 \bmod p = 1$, then $(a \bmod p)^2 = 1$, which is true only for $a \bmod p = 1$ or $a \bmod p = -1$.

The **second property** is stated as follows: Let p be a prime number greater than 2. We can then write $p - 1 = 2^k q$ with $k > 0$, q odd. Let a be any integer in the range $1 < a < p - 1$. Then one of the two following conditions is true.

1. a^q is congruent to 1 modulo p . That is, $a^q \bmod p = 1$, or equivalently, $a^q \equiv 1 \pmod{p}$.
2. One of the numbers $a^q, a^{2q}, a^{4q}, \dots, a^{2^{k-1}q}$ is congruent to -1 modulo p . That is, there is some number j in the range $(1 \leq j \leq k)$ such that $a^{2^{j-1}q} \bmod p = -1 \bmod p = p - 1$ or equivalently, $a^{2^{j-1}q} \equiv -1 \pmod{p}$.

Miller Rabin Algorithm (MLA)

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** $a^q \text{mod } n = 1$ **then** return("inconclusive");
4. **for** $j = 0$ **to** $k - 1$ **do**
5. **if** $a^{2^j q} \text{mod } n = n - 1$ **then** return("inconclusive");
6. **return**("composite");

Miller Rabin Algorithm (Proof)

Fermat's theorem states that $a^{n-1} \equiv 1 \pmod{n}$ if n is prime. We have $p - 1 = 2^k q$. Thus, we know that $a^{p-1} \pmod{p} = a^{2^k q} \pmod{p} = 1$. Thus, if we look at the sequence of numbers

$$a^q \pmod{p}, a^{2q} \pmod{p}, a^{4q} \pmod{p}, \dots, a^{2^{k-1}q} \pmod{p}, a^{2^k q} \pmod{p}$$

we know that the last number in the list has value 1. Further, each number in the list is the square of the previous number. Therefore, one of the following possibilities must be true.

1. The first number on the list, and therefore all subsequent numbers on the list, equals 1.
2. Some number on the list does not equal 1, but its square mod p does equal 1.
By virtue of the first property of prime numbers defined above, we know that the only number that satisfies this condition is $p - 1$. So, in this case, the list contains an element equal to $p - 1$.

This completes the proof.

MLA on 105

- $n = 105$
- $n-1 = 2^k * q$
- $104 = 2^3 * 13$; where $k=3$ and $q=13$
- Select $a = 2$
- $a^q \text{ mod } n = 2^{13} \text{ mod } 105 = 2$
- $a^{2*q} \text{ mod } n = (a^q \text{ mod } n)^2 \text{ mod } n = 2^2 \text{ mod } 105 = 4$
- $a^{4*q} \text{ mod } n = (a^{2*q} \text{ mod } n)^2 \text{ mod } n = 4^2 \text{ mod } 105 = 16$
- Hence, 105 is composite

MLA on 35

- $n = 35$
- $n-1 = 2^k * q$ i.e. $34 = 2^1 * 17$; where $k=1$ and $q=17$
- Select $a=2$
- $a^q \text{ mod } n = 2^{17} \text{ mod } 35 = 32$
- Hence 35 is composite

MLA on 233

- $n = 233$
- $n-1 = 2^k * q$ i.e. $232 = 2^3 * 29$; where $k=3$ and $q=29$
- Select $a = 2$
- $a^q \text{ mod } n = 2^{29} \text{ mod } 233 = 1$
- Hence, 233 is a prime

MLA on 61

- $n = 61$
- $n-1 = 2^k * q$ i.e. $60 = 2^2 * 15$; where $k=2$ and $q=15$
- Select $a = 2$
- $a^q \text{ mod } n = 2^{15} \text{ mod } 61 = 11$
- $a^{2*q} \text{ mod } n = (a^q \text{ mod } n)^2 \text{ mod } n = 11^2 \text{ mod } 61 = 60$
- Hence, 61 is prime

MLA on 241

- $n = 241$
- $n-1 = 2^k * q$ i.e. $240 = 2^4 * 15$; where $k=4$ and $q=15$
- Select $a = 2$
- $a^q \bmod n = 2^{15} \bmod 241 = 233$
- $a^{2*q} \bmod n = (a^q \bmod n)^2 \bmod n = 233^2 \bmod 241 = 64$
- $a^{4*q} \bmod n = (a^{2*q} \bmod n)^2 \bmod n = 64^2 \bmod 241 = 240$
- Hence, 241 is prime

CHINESE REMAINDER THEOREM (CRT)

CRT algorithm

- Let $m_1, m_2, m_3, \dots, m_k$ be pairwise relatively prime integers. If $a_1, a_2, \dots, a_k \in \mathbb{Z}$, then there exists $x \in \mathbb{Z}$, which satisfies the linear set of congruences:-

$$x \equiv a_1 \pmod{m_1}$$

$$x \equiv a_2 \pmod{m_2}$$

.....

$$x \equiv a_k \pmod{m_k}$$

where $M = m_1 * m_2 * \dots * m_k$

- $M_i = M/m_i$
- $x = (a_1 * M_1 * N_1 + a_2 * M_2 * N_2 + \dots + a_k * M_k * N_k) \pmod{M}$

where $N_i = MI(M_i) \pmod{m_i}$

CRT Example 1:-

- Solve for x:-

$$x \equiv 1 \pmod{5}$$

$$x \equiv 2 \pmod{6}$$

$$x \equiv 3 \pmod{7}$$

- $a_1 = 1, a_2 = 2, a_3 = 3, m_1 = 5, m_2 = 6, m_3 = 7;$
- $M = m_1 * m_2 * m_3 = 5 * 6 * 7 = 210$
- $M_1 = M/m_1 = 210/5 = 42$
- $M_2 = M/m_2 = 210/6 = 35$
- $M_3 = M/m_3 = 210/7 = 30$

CRT Example 1 (Contd..)

- $N_1 = MI(M_1) \pmod{m_1}$
- $N_1 = MI(42) \pmod{5}$

q	a	b	r	u1	u2	u
8	42	5	2	1	0	1
2	5	2	1	0	1	-2
2	2	1	0	1	-2	5
	1	0		-2	5	

- $N_1 = -2 \pmod{5} = 3$

CRT Example 1 (Contd..)

- $N_2 = MI(M_2) \pmod{m_2}$
- $N_2 = MI(35) \pmod{6}$

q	a	b	r	u1	u2	u
5	35	6	5	1	0	1
1	6	5	1	0	1	-1
5	5	1	0	1	-1	6
	1	0		-1	6	

- $N_2 = -1 \pmod{6} = 5$

CRT Example 1 (Contd..)

- $N_3 = MI(M_3) \pmod{m_3}$
- $N_3 = MI(30) \pmod{7}$

q	a	b	r	u1	u2	u
4	30	7	2	1	0	1
3	7	2	1	0	1	-3
2	2	1	0	1	-3	7
	1	0		-3	7	

- $N_3 = -3 \pmod{7} = 4$

CRT Example 1 (Contd..)

- $x = (a_1 * M_1 * N_1 + a_2 * M_2 * N_2 + a_3 * M_3 * N_3) \text{ mod } M$
- $x = (1 * 42 * 3 + 2 * 35 * 5 + 3 * 30 * 4) \text{ mod } 210 = 206$

CRT Example 2:-

- Solve for x:-

$x \equiv 3 \pmod{5}$
$x \equiv 4 \pmod{8}$
$x \equiv 11 \pmod{13}$
$x \equiv 6 \pmod{17}$

- $a_1 = 3, a_2 = 4, a_3 = 11, a_4 = 6$ $m_1 = 5, m_2 = 8, m_3 = 13, m_4 = 17;$
- $M = m_1 * m_2 * m_3 * m_4 = 5 * 8 * 13 * 17 = 8840$
- $M_1 = M/m_1 = 8840/5 = 1768$
- $M_2 = M/m_2 = 8840/8 = 1105$
- $M_3 = M/m_3 = 8840/13 = 680$
- $M_4 = M/m_4 = 8840/17 = 520$

CRT Example 2 (Contd..)

- $N_1 = MI(M_1) \pmod{m_1}$
- $N_1 = MI(1768) \pmod{5}$

q	a	b	r	u1	u2	u
353	1768	5	3	1	0	1
1	5	3	2	0	1	-1
1	3	2	1	1	-1	2
2	2	1	0	-1	2	-5
	1	0		2	-5	

- $N_1 = 2$

CRT Example 2 (Contd..)

- $N_2 = MI(M_2) \pmod{m_2}$
- $N_2 = MI(1105) \pmod{8}$

q	a	b	r	u1	u2	u
138	1105	8	1	1	0	1
8	8	1	0	0	1	-8
	1	0		1	-8	

- $N_2 = 1$

CRT Example 2 (Contd..)

- $N_3 = MI(M_3) \pmod{m_3}$
- $N_3 = MI(680) \pmod{13}$

q	a	b	r	u1	u2	u
52	680	13	4	1	0	1
3	13	4	1	0	1	-3
4	4	1	0	1	-3	13
	1	0		-3	13	

- $N_3 = -3 \pmod{13} = 10$

CRT Example 2 (Contd..)

- $N_4 = MI(M_4) \pmod{m_4}$
- $N_4 = MI(520) \pmod{17}$

q	a	b	r	u1	u2	u
30	520	17	10	1	0	1
1	17	10	7	0	1	-1
1	10	7	3	1	-1	2
2	7	3	1	-1	2	-5
3	3	1	0	2	-5	17
	1	0		-5	17	

- $N_4 = -5 \pmod{17} = 12$

CRT Example 2 (Contd..)

- $x = (a_1 * M_1 * N_1 + a_2 * M_2 * N_2 + a_3 * M_3 * N_3 + a_4 * M_4 * N_4) \text{ mod } M$
- $x = (3 * 1768 * 2 + 4 * 1105 * 1 + 11 * 680 * 10 + 6 * 520 * 12) \text{ mod } 8840 = 3508$

DISCRETE LOGARITHMS

Order of an Integer $a \bmod n$

- $\text{Order}_n(a) = \text{smallest natural number } k \text{ such that } a^k \bmod n = 1; \text{ where } \text{GCD}(a,n)=1, 1 \leq a < n, \text{ and } 1 \leq k \leq \phi(n).$
- $\text{Order}_7(2) = 3 \quad (2)^3 \bmod 7 = 1$
- $\text{Order}_5(3) = 4 \quad (3)^4 \bmod 5 = 1$
- $\text{Order}_{15}(8) = 4 \quad (8)^4 \bmod 15 = 1$
- $\text{Order}_9(8) = 2 \quad (8)^2 \bmod 9 = 1$
- $\text{Order}_8(1) = 1$

$\text{Ord}_9(4) = ?$

- $\text{GCD}(4,9) = 1$
- $4^1 \bmod 9 = 4$
- $4^2 \bmod 9 = 7$
- $4^3 \bmod 9 = 1$
- Therefore $\text{Ord}_9(4) = 3$

$\text{Ord}_{11}(8) = ?$

- $\text{GCD}(8,11) = 1$
- $\phi(11) = 10$
- $8^1 \bmod 11 = 8$
- $8^2 \bmod 11 = 9$
- $8^3 \bmod 11 = 6$
- $8^4 \bmod 11 = 4$
- $8^5 \bmod 11 = 10$
- $8^6 \bmod 11 = 3$
- $8^7 \bmod 11 = 2$
- $8^8 \bmod 11 = 5$
- $8^9 \bmod 11 = 7$
- $8^{10} \bmod 11 = 1$
- Therefore $\text{Ord}_{11}(8) = 10$

$$\text{Ord}_{12}(8) = ?$$

- 
- $\text{GCD}(8,12) = 4$.
 - Therefore $\text{Ord}_{12}(8)$ doesn't exist.

Primitive Roots of n

- ‘a’ is a primitive root of n if $\text{Ord}_n(a) = \phi(n)$.
- All n don’t have primitive roots. For n to have primitive roots, $n=2, 4, p^\alpha, 2*p^\alpha$, where p is any odd prime, α is a natural number
- Examples of natural numbers having primitive roots are 2,3,4,5,6,7,9,10,11, etc.
- Examples of natural numbers which don’t have primitive roots are 8, 12, 15, etc.
- Primitive roots of 7 are 3 and 5.
- Primitive roots of 5 are 2 and 3.

Primitive Roots of 11

- $\phi(11) = 10$

a=1:-

- $1^1 \bmod 11$
- $\text{Ord}_{11}(1) = 1$
- Hence 1 is not a primitive root of 11

a=2:-

- $2^1 \bmod 11 = 2$
- $2^2 \bmod 11 = 4$
- $2^3 \bmod 11 = 8$
- $2^4 \bmod 11 = 5$
- $2^5 \bmod 11 = 10$
- $2^6 \bmod 11 = 9$

Primitive Roots of 11 (Contd..)

- $2^7 \bmod 11 = 7$
- $2^8 \bmod 11 = 3$
- $2^9 \bmod 11 = 6$
- $2^{10} \bmod 11 = 1$
- $\text{Ord}_{11}(2) = 10$
- Hence 2 is a primitive root of 11

a=3:-

- $3^1 \bmod 11 = 3$
- $3^2 \bmod 11 = 9$
- $3^3 \bmod 11 = 5$
- $3^4 \bmod 11 = 4$
- $3^5 \bmod 11 = 1$
- $\text{Ord}_{11}(3) = 5$
- Hence, 3 is not a primitive root of 11

Primitive Roots of 11 (Contd..)

a=4:-

- $4^1 \bmod 11 = 4$
- $4^2 \bmod 11 = 5$
- $4^3 \bmod 11 = 9$
- $4^4 \bmod 11 = 3$
- $4^5 \bmod 11 = 1$
- $\text{Ord}_{11}(4) = 5$
- Hence 4 is not a primitive root of 11

a=5:-

- $\text{Ord}_{11}(5) = 5$
- Hence , 5 is not a primitive root of 11.

Primitive Roots of 11 (Contd..)

a=6:-

- $\text{Ord}_{11}(6) = 10$
- Hence , 6 is a primitive root of 11.

a=7:-

- $\text{Ord}_{11}(7) = 10$
- Hence , 7 is a primitive root of 11.

a=8:-

- $\text{Ord}_{11}(8) = 10$
- Hence , 8 is a primitive root of 11.

Primitive Roots of 11 (Contd..)

a=9:-

- $\text{Ord}_{11}(9) = 5$
- Hence , 9 is not a primitive root of 11.

a=10:-

- $\text{Ord}_{11}(10) = 2$
- Hence , 10 is not a primitive root of 11.

- Therefore, the primitive roots of 11 are 2, 6, 7, and 8

Primitive Roots of 2

- $n = 2$
- $\phi(2) = 1$
- $1^1 \bmod 2 = 1$
- Hence, $\text{Ord}_2(1) = 1$
- The primitive root of 2 is 1.

Primitive Roots of 4

- $n = 4$
- $\phi(4) = 2$
- $\text{Ord}_4(1) = 1$
- $\text{GCD}(2,4) = 2$; Hence 2 can't be a primitive root of 4
- $\text{Ord}_4(3) = 2$
- Hence 3 is a primitive root of 4

Primitive Roots of 9

- $n = 9 = 3^2$; Here $p = 3$, and $\alpha=2$
- $\phi(9) = 3^2 - 3 = 6$
- $\text{Ord}_9(1) = 1$
- $\text{Ord}_9(2) = 6$; Hence 2 is a primitive root
- $\text{GCD}(3,9) = 3$
- $\text{Ord}_9(4) = 3$
- $\text{Ord}_9(5) = 6$; Hence 5 is a primitive root
- $\text{GCD}(6,9) = 3$
- $\text{Ord}_9(7) = 3$
- $\text{Ord}_9(8) = 2$
- The primitive roots of 9 are 2 and 5.

Primitive Roots of 20

- 20 cannot be expressed as p^α or $2 * p^\alpha$
- Hence 20 doesn't have any primitive root.

Observations Regarding Primitive Roots

- If \mathbf{a} is a primitive root of n , then the set $\{a^1, a^2, \dots, a^{\phi(n)}\} \pmod{n}$ contain unique elements and are relatively prime to n .
- For example, the set $\{2^1, 2^2, 2^3, 2^4, 2^5, 2^6\} \pmod{9} = \{2, 4, 8, 7, 5, 1\}$ contains unique elements which are relatively prime to 9.

Discrete Logarithms

- If $b = a^x \text{ mod } n$, then discrete logarithm is given by $x = \text{dlog}_{a,n}(b)$, where $\text{GCD}(b,n) = 1$ and ‘a’ is a primitive root of n.
- Calculating Discrete Logarithms is a relatively harder problem than exponentiation.

Calculate the Discrete logarithm x, where $3^x \text{ mod } 7 = 4$:

- $\text{GCD}(4,7) = 1$
- $\text{Ord}_7(3) = 6$;
- Min value of x = 4.
- Therefore, $x = 4 + 6 * k$, where $k \in \mathbb{W}$.

Solve for x:- $5^x \pmod{18} = 11$

- $\text{GCD}(11,18) = 1$
- $\text{Ord}_{18}(5) = 6$
- Min value of x = 5
- Therefore, $x = 5 + 6*k$, where $k \in \mathbb{W}$.

PRINCIPLES OF CRYPTOGRAPHY

CSE 3121

What's Computer Security

- Also known as Cyber Security
- Practice of Protection of stored and transmitted data
- Used to preserve different security goals (Confidentiality, Integrity, Availability, etc.) of the data from an adversary or a group of adversaries.



Syllabus

Security Goals, Attacks, Services, Mechanisms, Symmetric Cipher Model, Block Ciphers and DES, Strength of DES, Block Cipher Design Principles. AES, Equivalent Inverse Cipher. Block Cipher Operation- Multiple Encryption and Triple DES, Electronic Codebook, Cipher Block Chaining Mode, Cipher Feedback Mode, Output Feedback Mode, Counter Mode, XTS-AES Mode for Block-Oriented Storage Devices, Format-Preserving Encryption. Euclidean Algorithm, Modular Arithmetic, Prime Numbers, Fermat and Euler theorems, Testing for Primality, Chinese Remainder theorem, Discrete Logarithms. Pseudorandom Number Generation, Stream Ciphers, RC4. Public Key Cryptography and RSA. D-H Key Exchange, ElGamal System. Cryptographic Hash Functions. Message Authentication Codes, Security of MACs, HMAC.

Textbooks

1. William Stallings, Cryptography and Network Security: Principles and Practice, (7e), Prentice Hall, 2017.
2. Behrouz A. Forouzan and Debdeep Mukhopadhyay, Cryptography and Network Security, (2e), McGraw Hill, 2008
3. Atul Kahate, Cryptography and Network Security, Tata McGraw-Hill Publishing, 2008
4. Bruce Schneier, Applied Cryptography-Protocols, Algorithms, and source code in C, (2e), John Wiley & Sons, Inc., 2013

CO

- CO1: Illustrate the cryptographic attacks, services, and classical symmetric ciphers
- CO2: Analyze the various block ciphers and modes of operation.
- CO3: Utilize the concepts of number theory and pseudo random number generation.
- CO4: Explain public key crypto system.
- CO5: Apply various data integrity algorithms

SECURITY GOALS

Security goals defined by FIPS 199

- FIPS (Standards for Security Categorization of Federal Information and Information Systems)
- CIA Triad defined by FIPS



Confidentiality ()

- Ensures that sensitive information is accessed only by authorized individuals, entities, or processes.
- It protects data from unauthorized disclosure.

Integrity (✓)

- Ensures that data is not tampered with and remains in its original state, providing assurance that the information is trustworthy and accurate.
- Data can be changed only by authorized entities.

Availability ()

- Ensures that information, systems, and services are accessible and usable upon demand by authorized users.
- Timely access to Google Drive, One Drive backups, etc.

2 Additional Security Goals

Authenticity (🔑):-

- Ensures that an entity (user, device, or system) is who or what it claims to be.
- Some examples could be Password based, Biometric based, etc.

Accountability (📋):-

- Mechanisms which ensure that individuals or communicating entities can be held responsible for their actions.

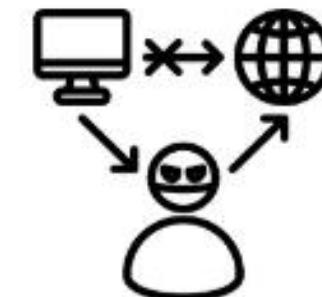
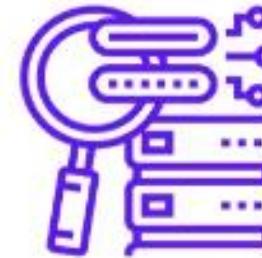
SECURITY ATTACKS

Security Attacks

Active Attacks



Passive Attacks

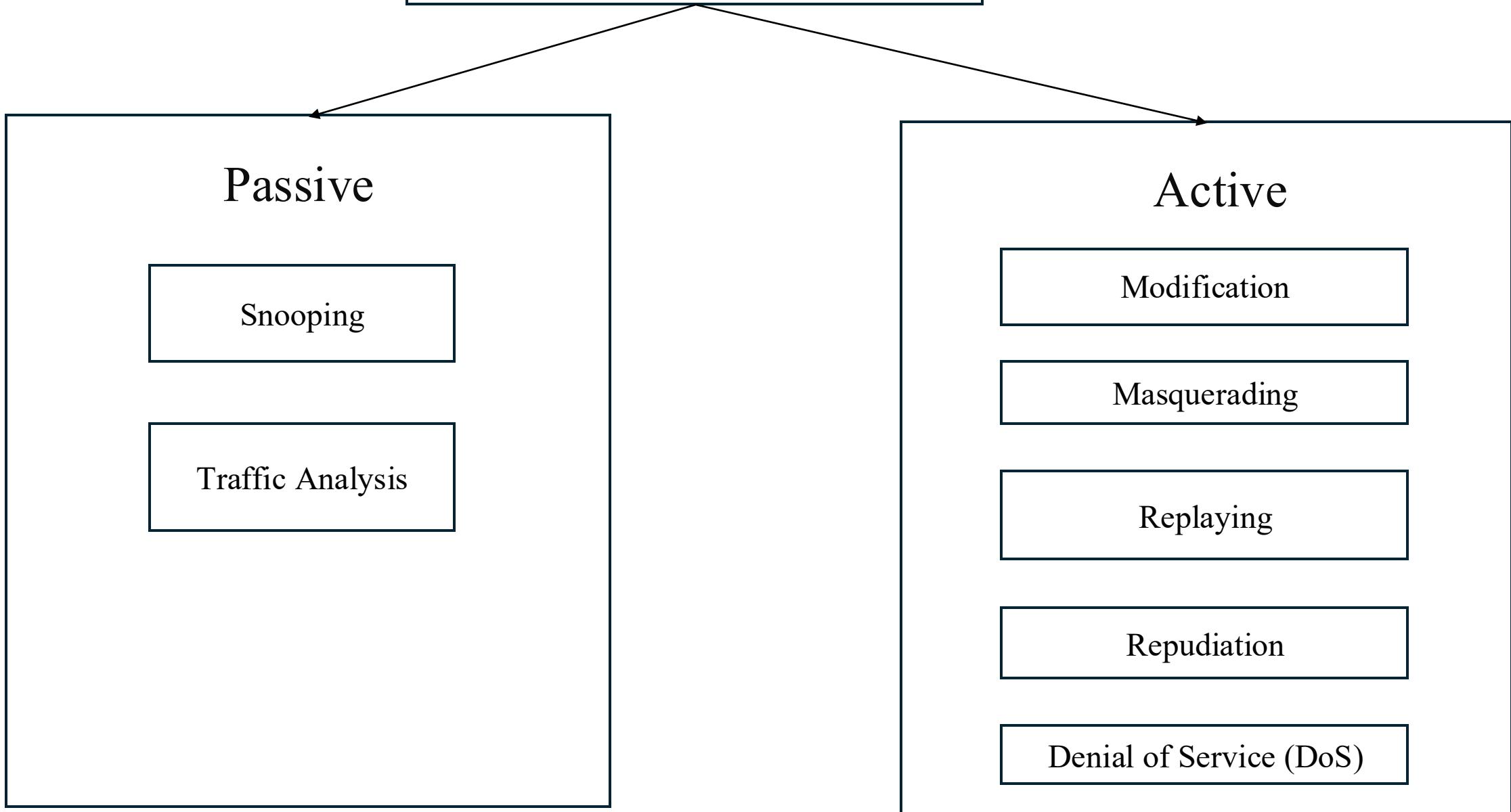


Insecure Lab

Security Attacks

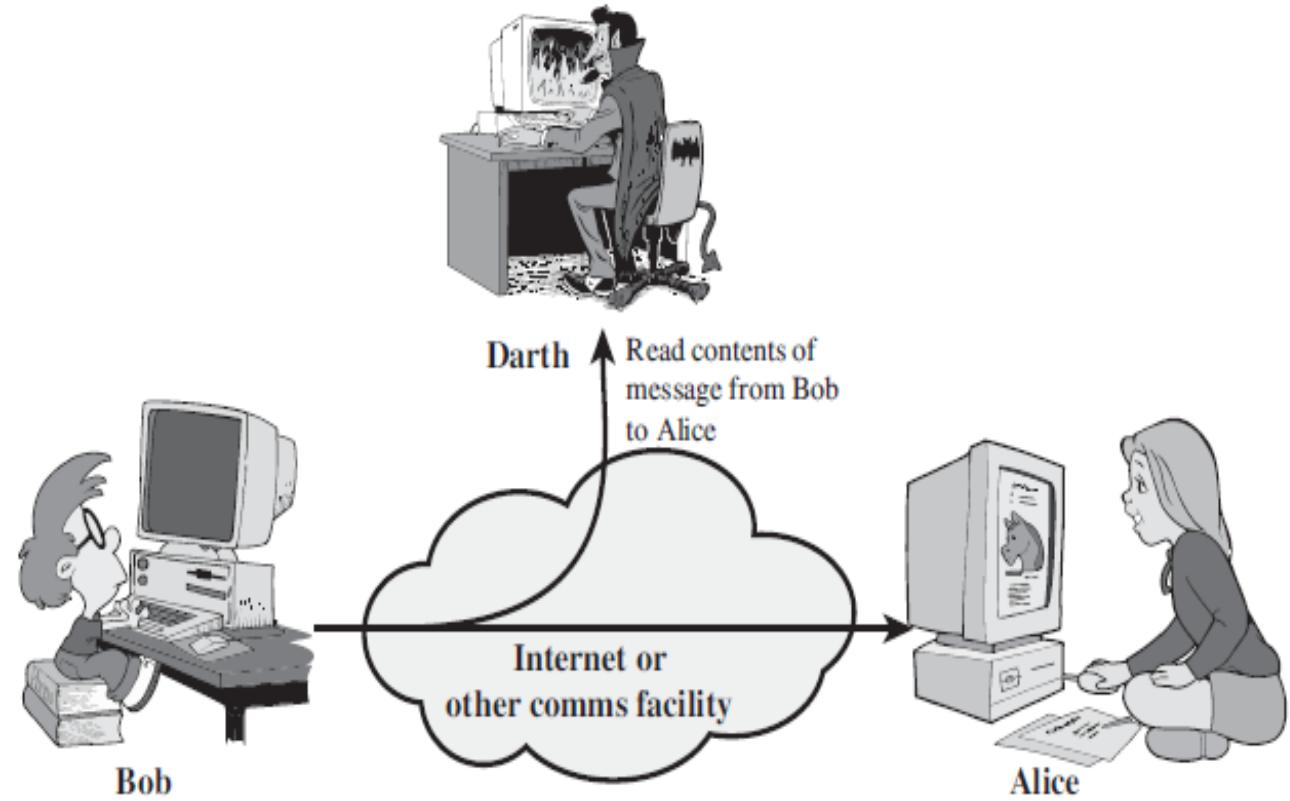
- A useful means of classifying security attacks
 - **Passive attacks:** A passive attack attempts to learn or make use of information from the system **but does not affect system resources.**
 - **Active attacks:** An active attack attempts to alter system resources or **affect their operation**

Security Attacks



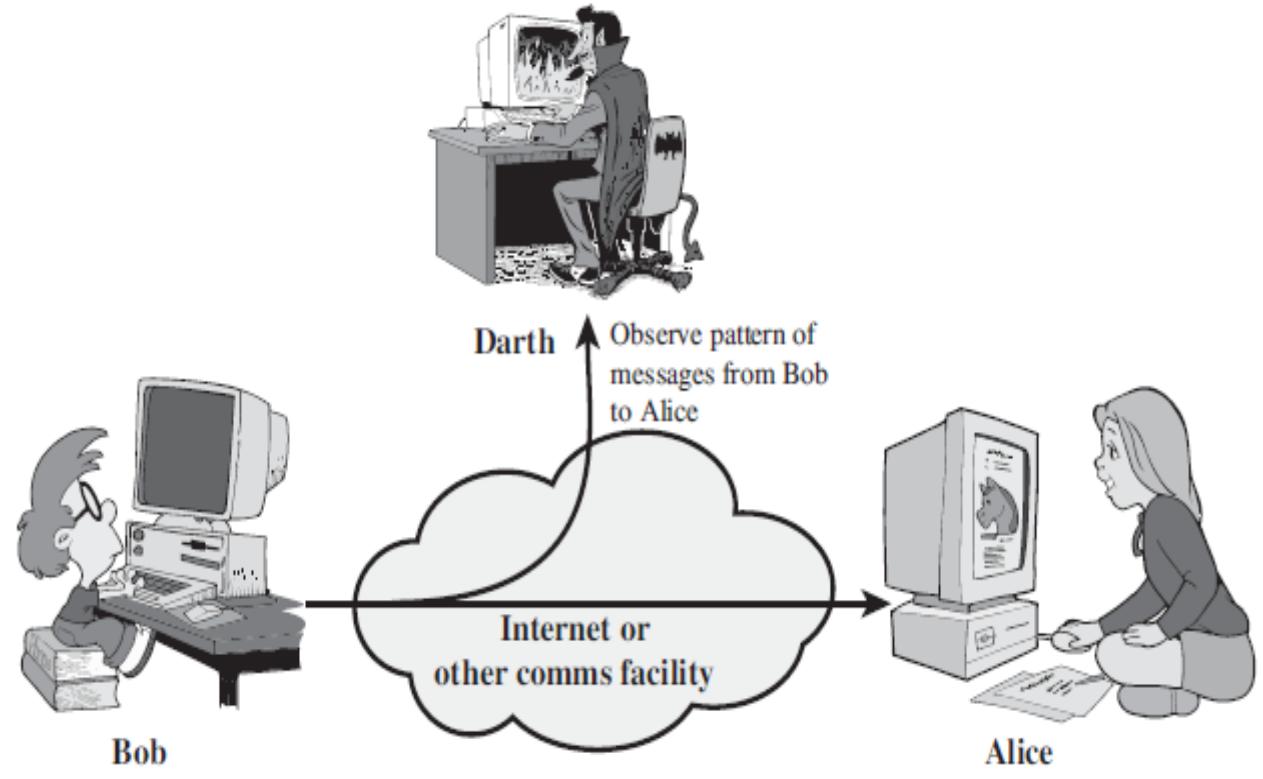
Snooping

- Captures and reads sensitive data transmitted across a network.
- The attacker concentrates on contents of the data.



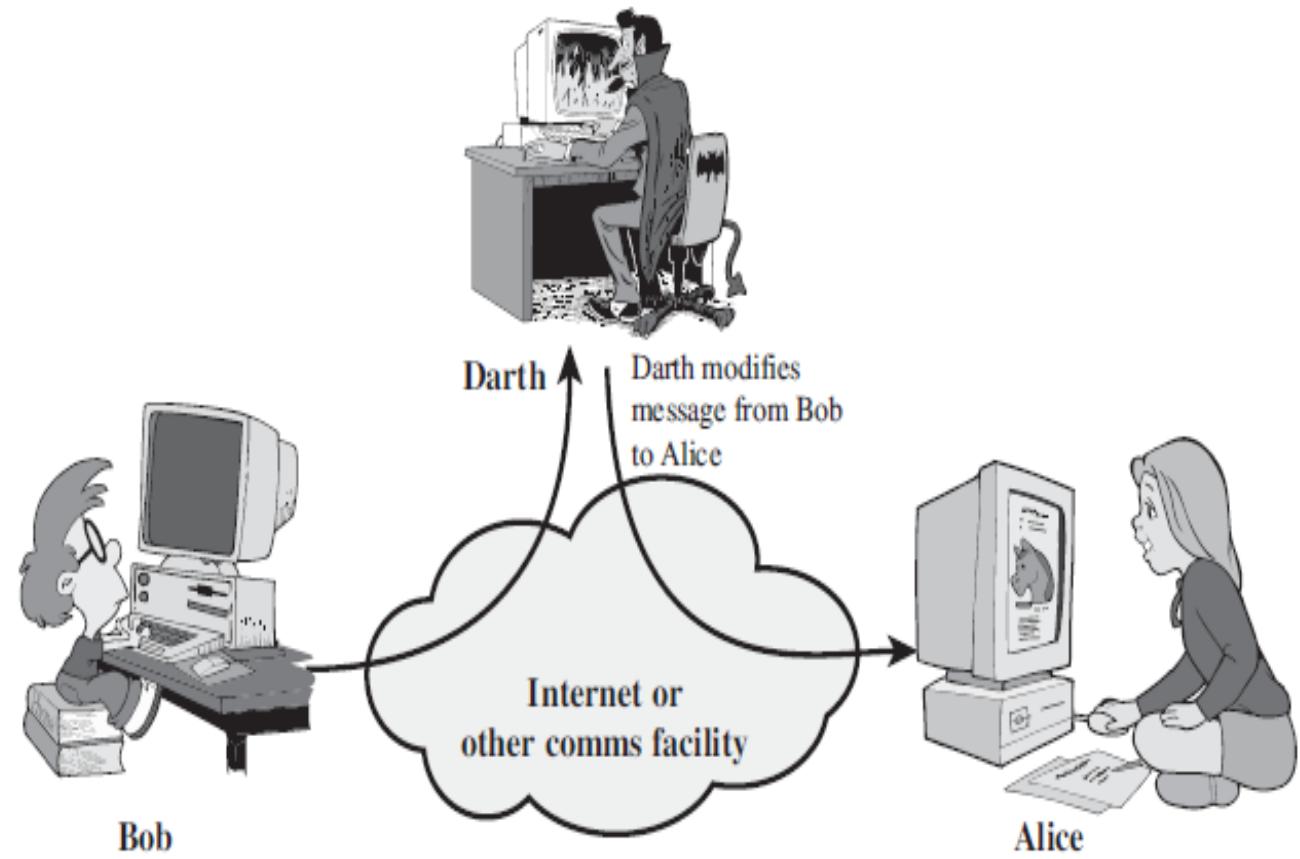
Traffic Analysis

- The attacker collects information and analyzes the network communication patterns.
- Concentrates on Metadata and traffic flow in a network.



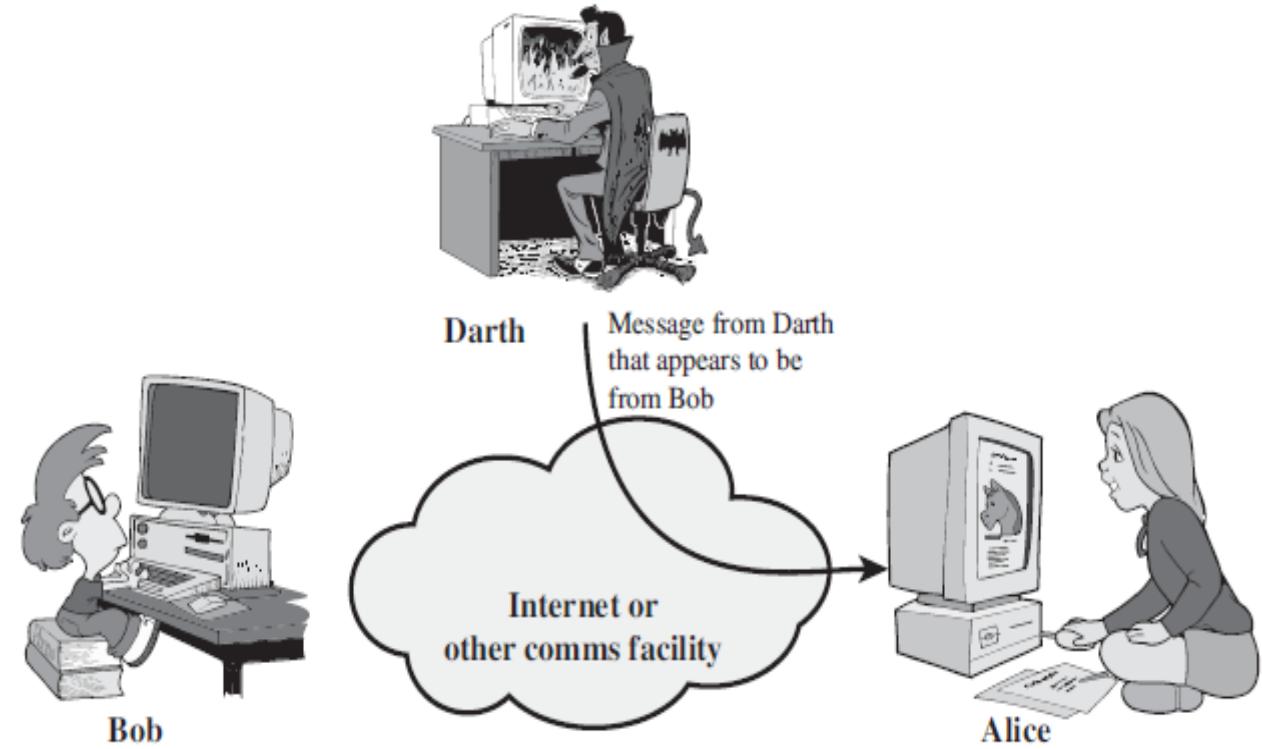
Modification

- Unauthorized manipulation, tampering, etc., of the legitimate data communicated over a network.



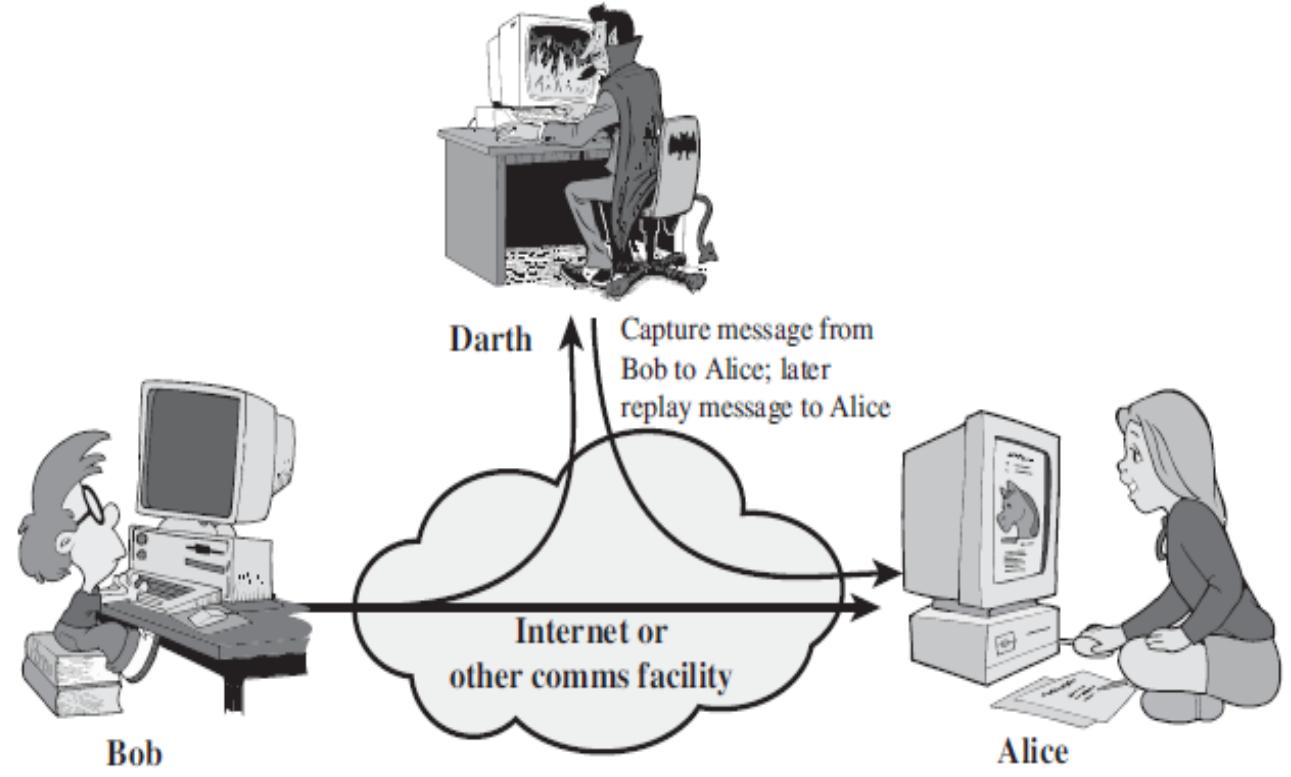
Masquerading

- Attacker pretends to be a legitimate entity to other legitimate entities in a network.



Replaying

- Subsequent retransmissions of a previously captured data packet.



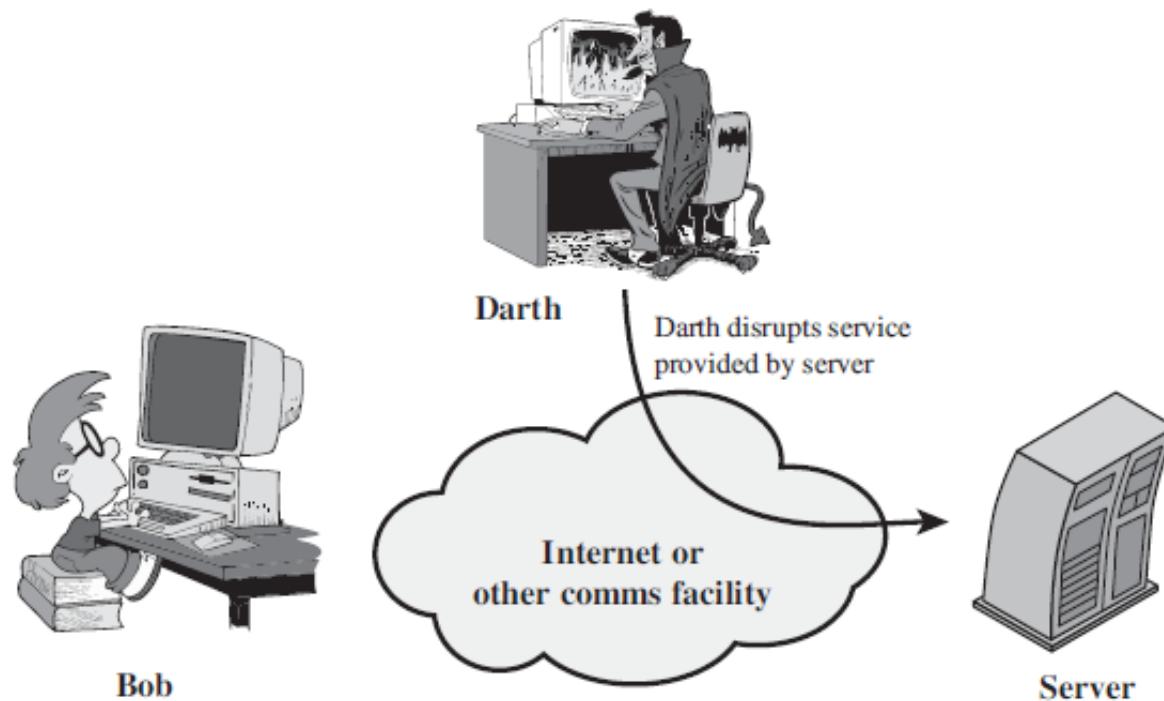
Repudiation

- Denying the fact that an entity was involved in a data communication.



DoS

- The attacker degrades a computer network by overloading it with unnecessary data traffic.



Passive Attacks

- Eavesdropping and/or Collecting Data
- Zero/Negligible impact on the system operations and/or the network performance.
- Comparatively harder to detect

Active Attacks

- Altering/Manipulating Data
- Major impact on the system operations and/or the network performance
- Comparatively easier to detect

SECURITY SERVICES

Security Services

Peer Entity Authentication

Data Origin Authentication

Access Control

Confidentiality

Data Integrity

Non-Repudiation

Availability

Security Services (Contd..)



Peer Entity Authentication:- Verification of the identities of the communicating entities.



Data Origin Authentication:- Verification of the source of the data, and that it is from a legitimate communicating entity.



Access Control:- Mechanisms and Policies which are defined to manage and restrict access to resources and data.



Confidentiality:- Includes 4 types of Confidentiality (Connection Confidentiality, Connectionless Confidentiality, Selective-Field Confidentiality, and Traffic Flow Confidentiality)

Security Services (Contd..)



Data Integrity:- Involves 5 types (Connection Integrity with Recovery, Connection Integrity without Recovery, Selective-Field Connection Integrity, Connectionless Integrity, and Selective-Field Connectionless Integrity)



Non-Repudiation:- 2 types (for Origin, and for Destination)



Availability

SECURITY MECHANISMS

Security Mechanisms

Encipherment

Digital Signature

Access Control

Data Integrity

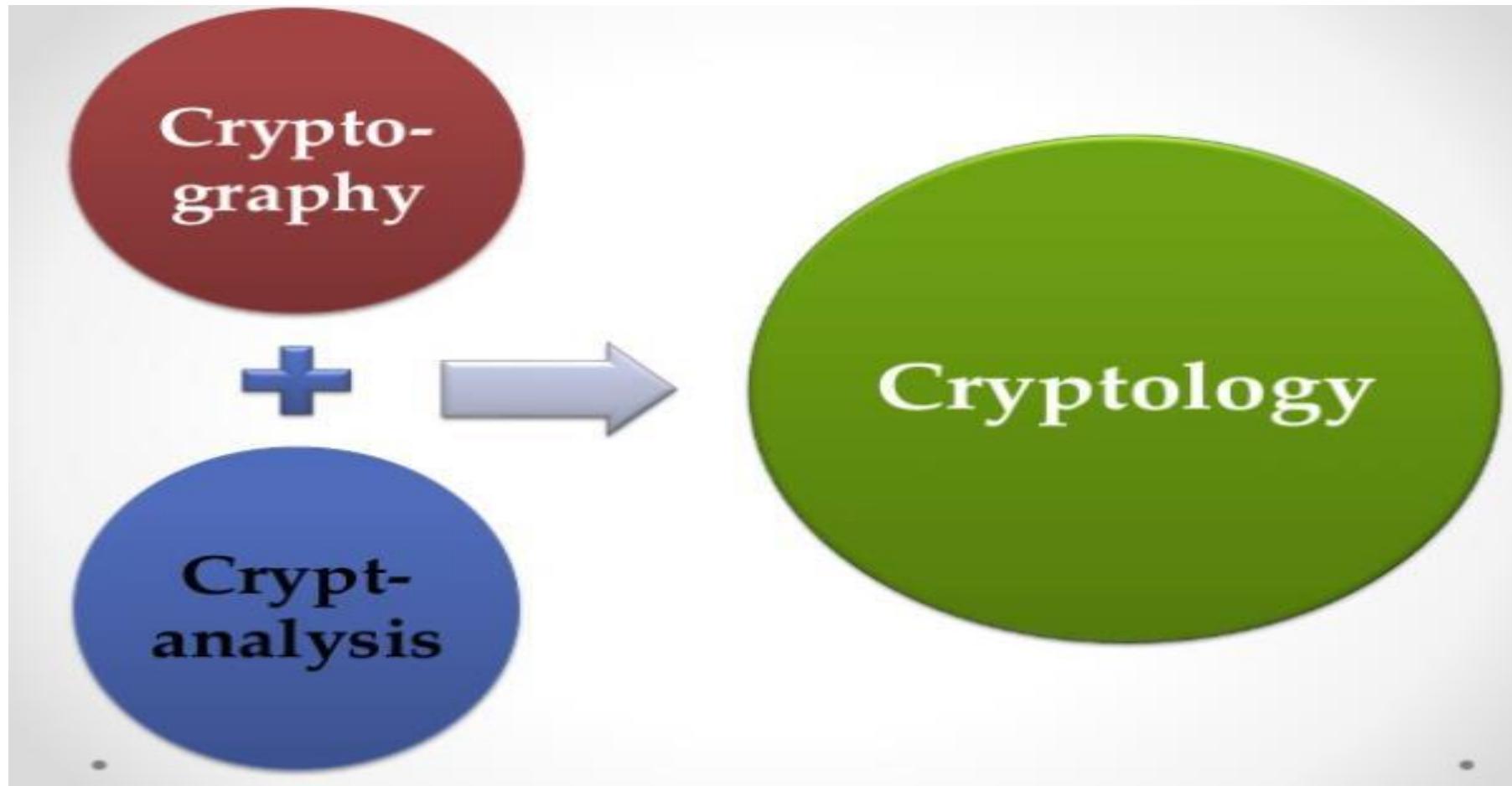
Authentication Exchange

Traffic Padding

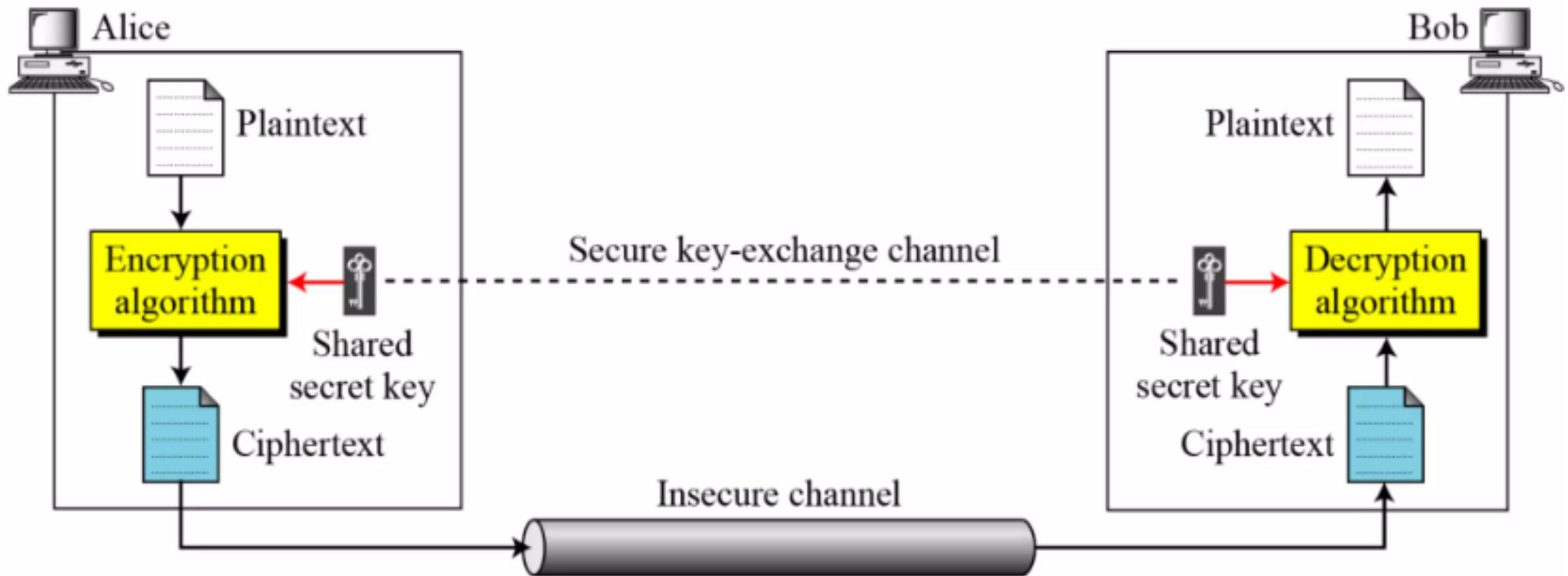
Routing Control

Notarization

What's Cryptography?



Symmetric Cipher Model



Symmetric Cipher Model (Contd..)

- Alice:- $C = E_k(P)$
- Bob:- $D = D_k(C) = D_k(E_k(P))$



Kerckhoff's Principle

- Published by Auguste Kerckhoff in 1883.
- Uses 2 key principles:- Algorithm Transparency, and Key Secrecy

3 Independent Dimensions of Cryptographic Systems

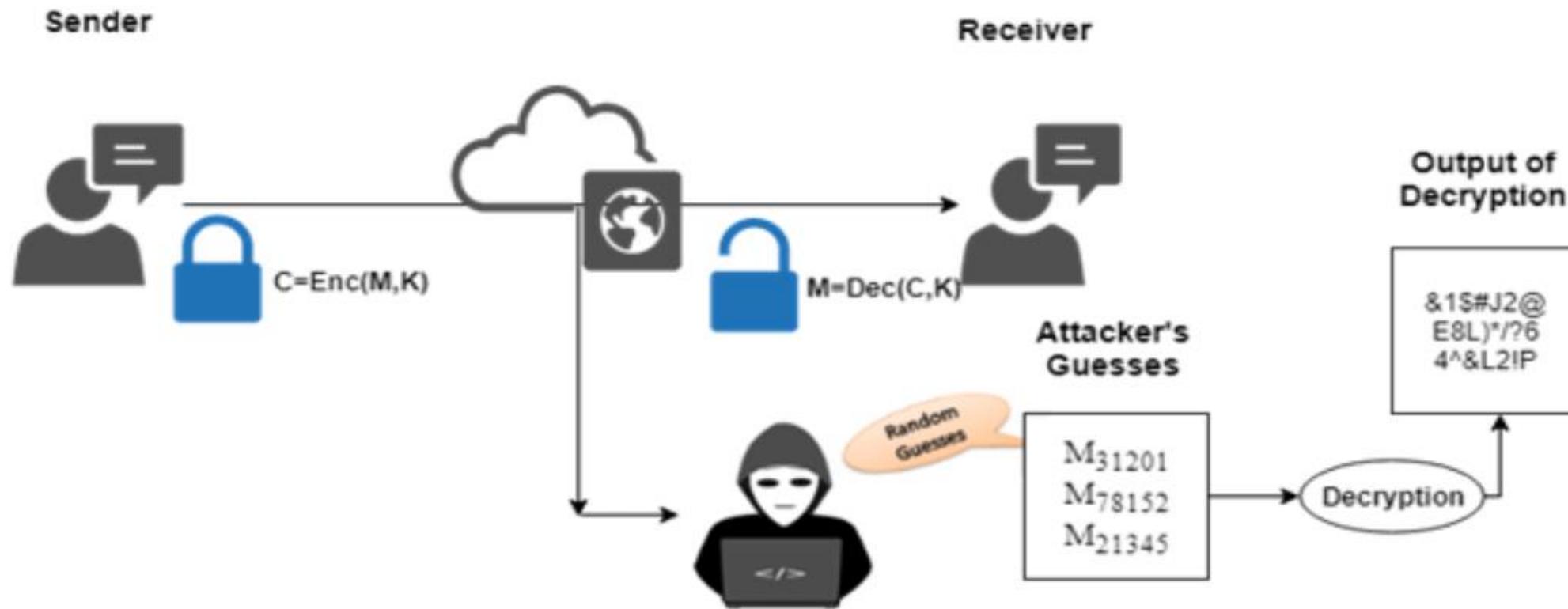
- Types of Operations used for transformation of PT to CT
- Number of keys used
- How PT is processed

CRYPTANALYSIS

Cryptanalysis Techniques on Encrypted Data

- 1) Brute Force Attack (BFA)
- 2) Statistical Attack
- 3) Pattern Attack
- 4) Ciphertext Only Attack
- 5) Known Plaintext Attack
- 6) Chosen Plaintext Attack
- 7) Chosen Ciphertext Attack

BFA



Statistical Attack

CT:- **wklwwewv ugddwyw**

- The letter ‘e’ is the most frequently used English alphabet for plaintext.
- Hence, for the above CT, the attacker makes a best case guess that most probably the ciphertext character ‘w’ maps to the plaintext character ‘e’.

Statistical Attack (Contd..)

Letter	Frequency	Letter	Frequency
e	12.7020%	m	2.4060%
t	9.0560%	w	2.3600%
a	8.1670%	f	2.2280%
o	7.5070%	g	2.0150%
i	6.9660%	y	1.9740%
n	6.7490%	p	1.9290%
s	6.3270%	b	1.4920%
h	6.0940%	v	0.9780%
r	5.9870%	k	0.7720%
d	4.2530%	j	0.1530%
l	4.0250%	x	0.1500%
c	2.7820%	q	0.0950%
u	2.7580%	z	0.0740%

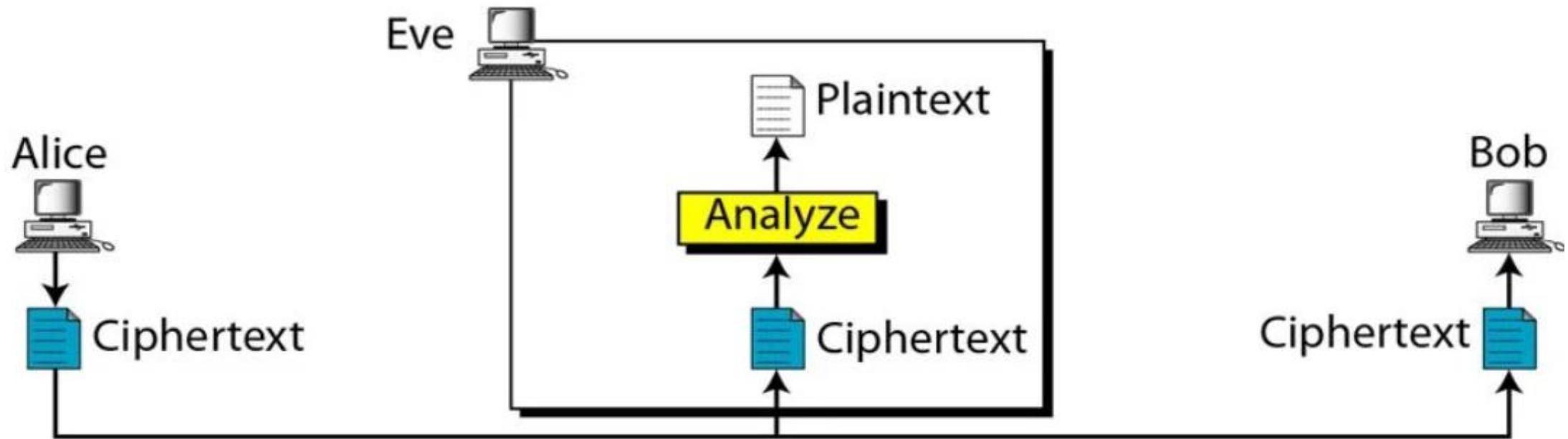
Pattern Attack

"KHOOR ZRUOG"

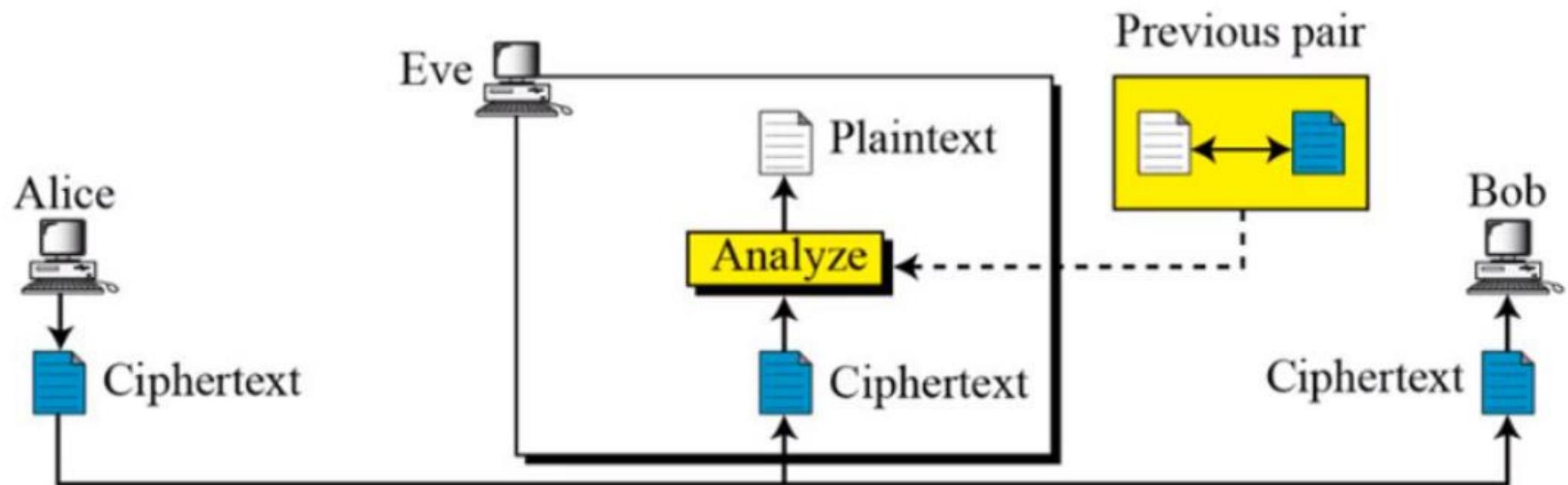


"HELLO WORLD"

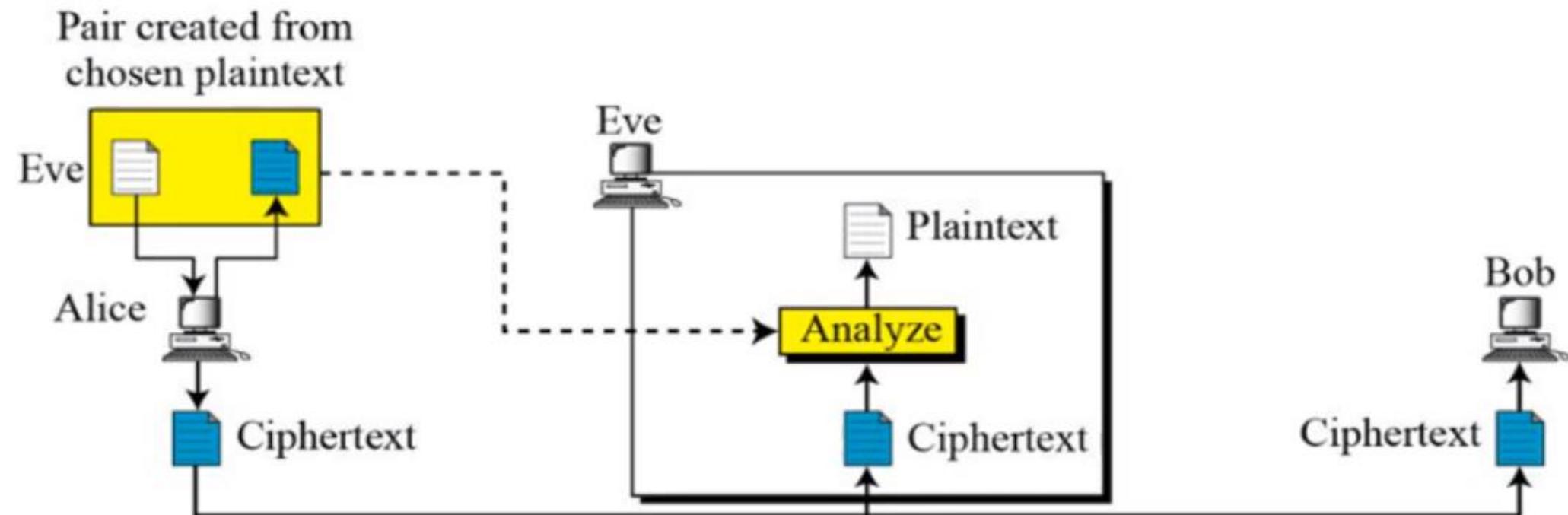
Ciphertext Only Attack



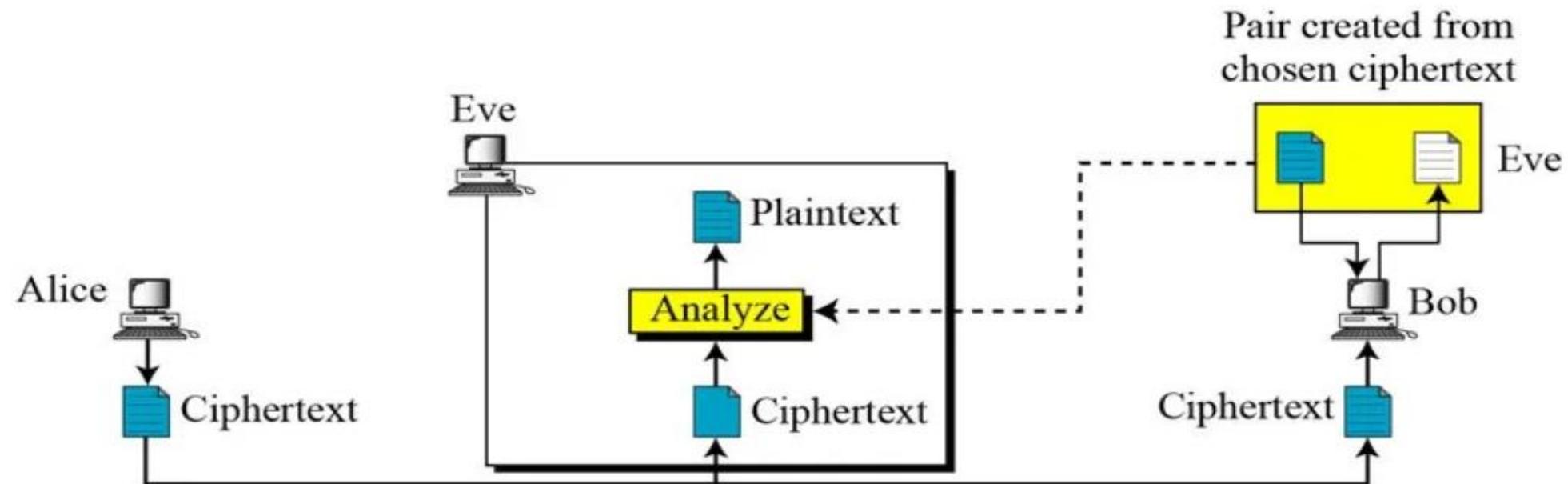
Known Plaintext Attack



Chosen Plaintext Attack

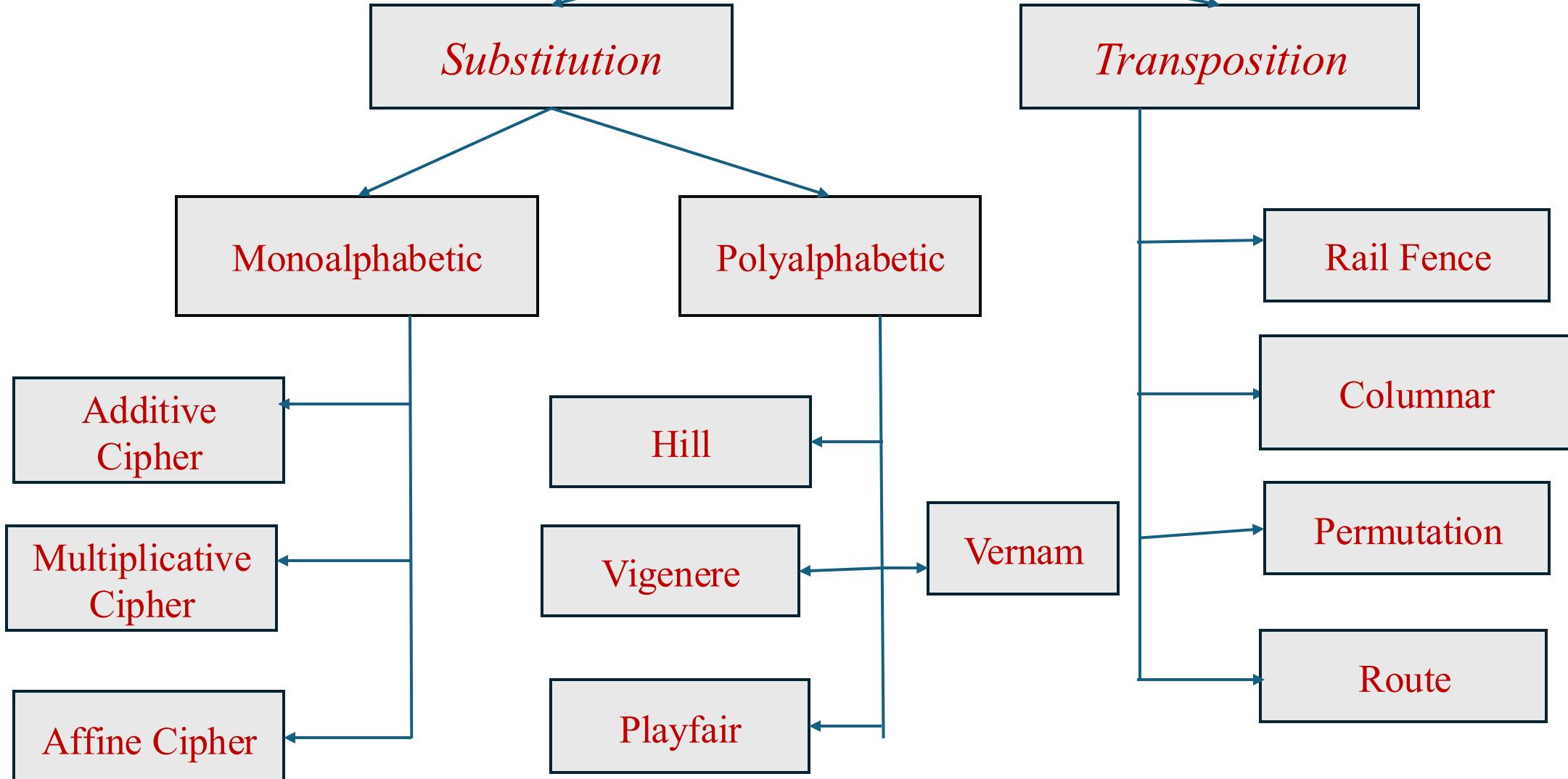


Chosen Ciphertext Attack



HIERARCHY OF CLASSICAL CIPHERS

Classical Ciphers

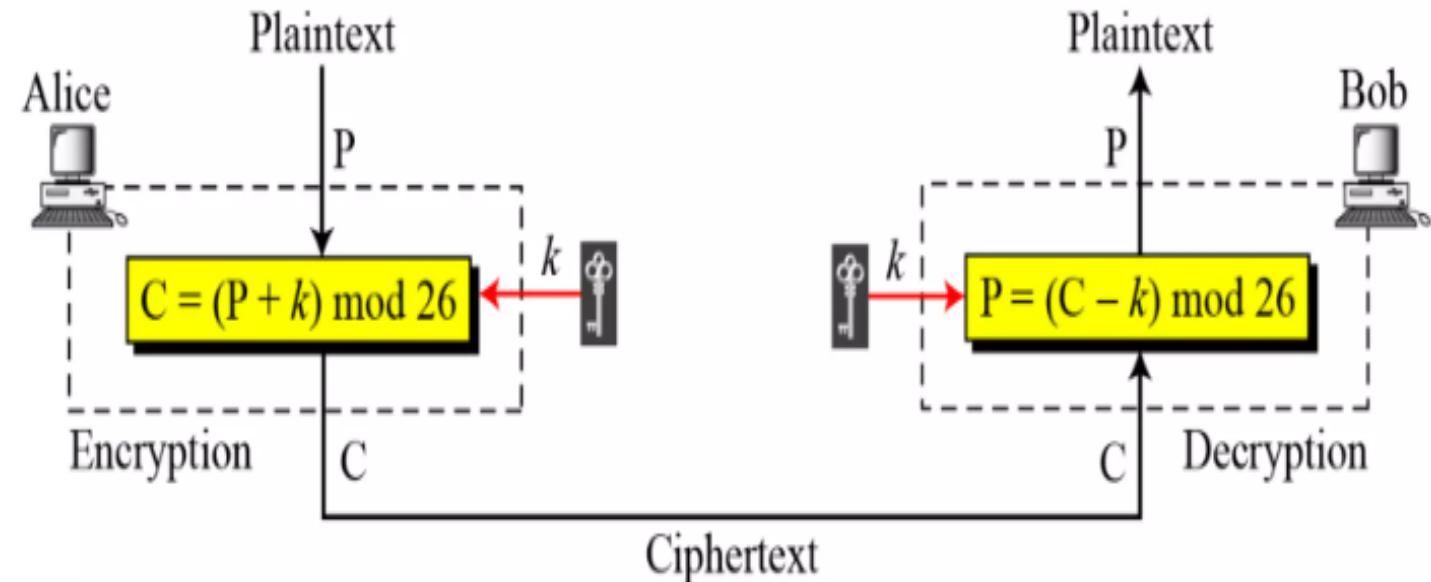


Default Numerical Values

Character	Numerical Equivalent	Character	Numerical Equivalent
a	0	n	13
b	1	o	14
c	2	p	15
d	3	q	16
e	4	r	17
f	5	s	18
g	6	t	19
h	7	u	20
i	8	v	21
j	9	w	22
k	10	x	23
l	11	y	24
m	12	z	25

ADDITIVE CIPHER

Additive Cipher

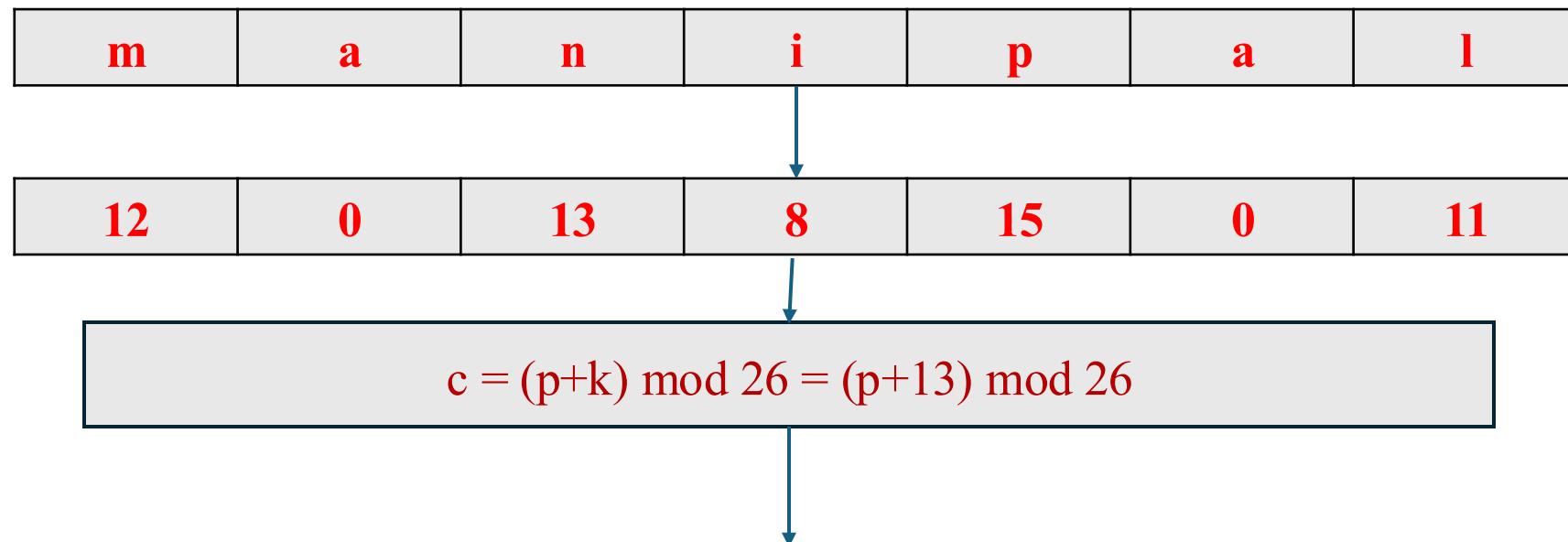


- Also called as Shift cipher.
- Here the key, PT and CT are in Z_{26} .

Example 1

Encrypt the message “manipal” using key = 13, and additive cipher in Z_{26} . Assume that the alphabets are case-insensitive and use the default numerical equivalents.

Solution:-



Example 1 (Contd..)

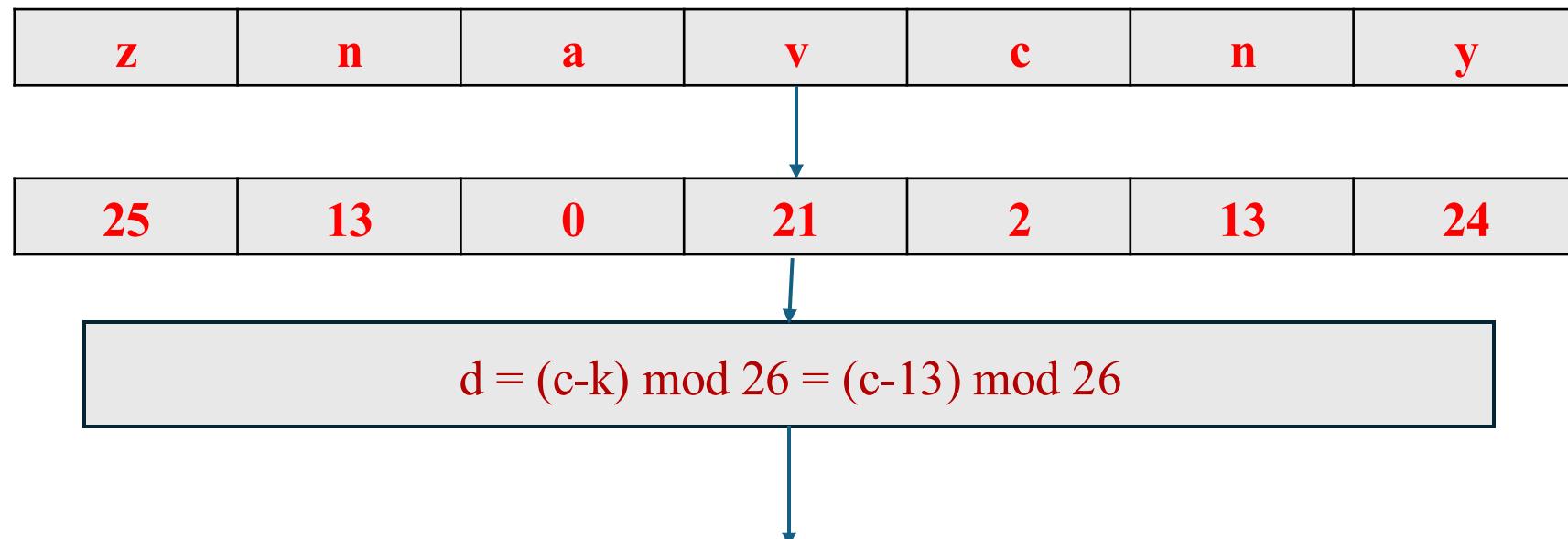
25	13	0	21	2	13	24
z	n	a	v	c	n	y

- Therefore, the encrypted message is “**znavcny**”.

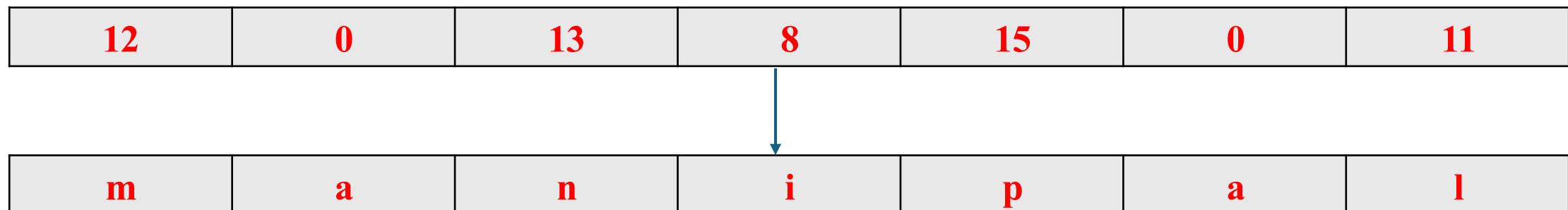
Example 2

Decrypt the message “znavcny” using key = 13, and additive cipher in Z_{26} . Assume that the alphabets are case-insensitive and use the default numerical equivalents.

Solution:-



Example 2 (Contd..)



- Therefore, the decrypted message is “**manipal**”.

Example 3

Assume that Additive cipher is used with some special characters with their corresponding numerical equivalents as displayed in the table below. Assume that the alphabets which are used are case-insensitive and use the default numerical equivalents. Decrypt the ciphertext “>d@a\\$d>>h\\$d@a>w” using key = 23.

Special Characters	Numerical Equivalents
?	26
>	27
<	28
@	29
#	30
\$	31
!	32

Example 3 (Solution)

- $> (27) \rightarrow \{d = (c-23) \bmod 33\} \rightarrow 4 \text{ (e)}$
- $d (3) \rightarrow \{d = (c-23) \bmod 33\} \rightarrow 13 \text{ (n)}$
- $@ (29) \rightarrow \{d = (c-23) \bmod 33\} \rightarrow 6 \text{ (g)}$
- $\$ (31) \rightarrow \{d = (c-23) \bmod 33\} \rightarrow 8 \text{ (i)}$
- $d (3) \rightarrow \{d = (c-23) \bmod 33\} \rightarrow 13 \text{ (n)}$
- $> (27) \rightarrow \{d = (c-23) \bmod 33\} \rightarrow 4 \text{ (e)}$
- $> (27) \rightarrow \{d = (c-23) \bmod 33\} \rightarrow 4 \text{ (e)}$

Example 3 (Solution)

- $h(7) \rightarrow \{d = (c-23) \bmod 33\} \rightarrow 17 \text{ (r)}$
- $\$(31) \rightarrow \{d = (c-23) \bmod 33\} \rightarrow 8 \text{ (i)}$
- $d(3) \rightarrow \{d = (c-23) \bmod 33\} \rightarrow 13 \text{ (n)}$
- $@(29) \rightarrow \{d = (c-23) \bmod 33\} \rightarrow 6 \text{ (g)}$
- $w(22) \rightarrow \{d = (c-23) \bmod 33\} \rightarrow 32 \text{ (!)}$
- Therefore, the decrypted text is “engineering!”

Digrams on Additive Ciphers

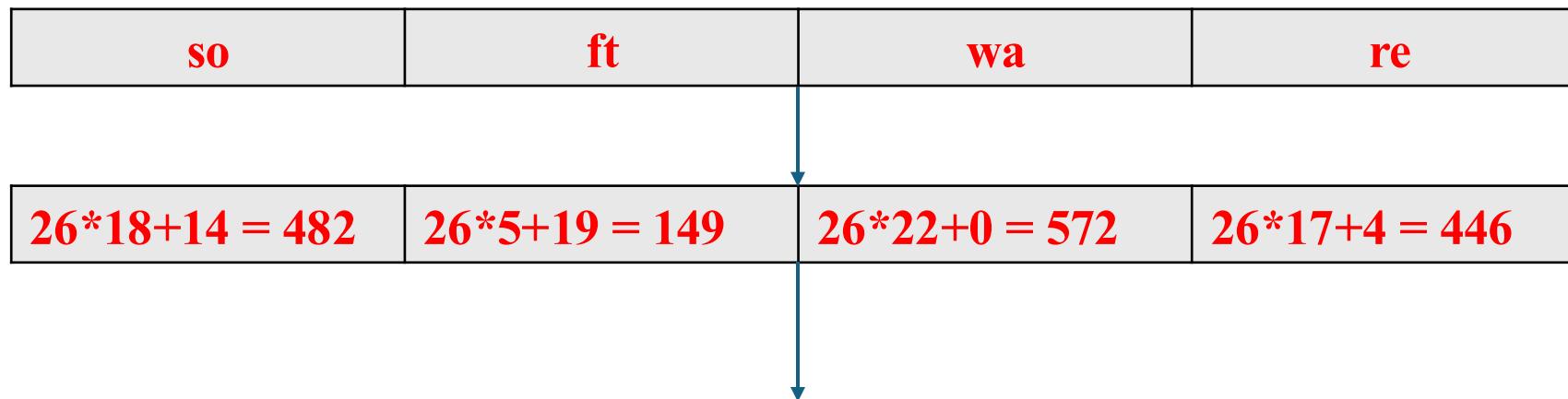
- Pairs of alphabets or characters are encrypted or decrypted.
- Most commonly used digrams in plaintexts are ‘th’, ‘he’, ‘in’, etc.
- $c = (p+k) \text{ mod } 676$, when only alphabets are used by ignoring the case.
- $d = (c-k) \text{ mod } 676$, when only alphabets are used by ignoring the case.

Additive Cipher with digram (Example 1)

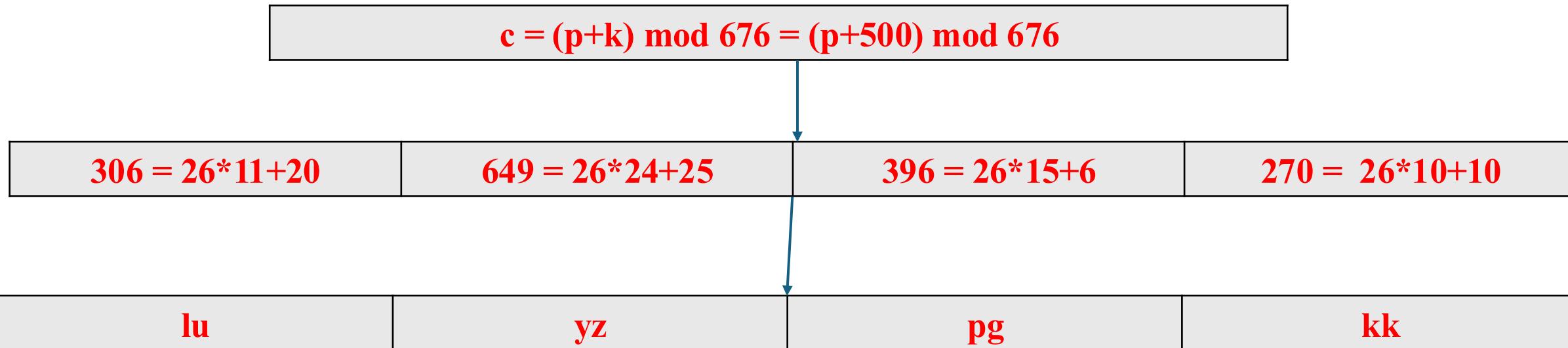
Encrypt the message “**software**” using key = 500, and additive cipher using digrams. Assume that the alphabets are case-insensitive and use the default numerical equivalents.

Solution:-

so	ft	wa	re
$26*18+14 = 482$	$26*5+19 = 149$	$26*22+0 = 572$	$26*17+4 = 446$



Additive Cipher with digram (Example 1) (Contd..)



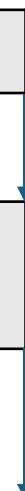
- The ciphertext is “**luyzpgkk**”.

Additive Cipher with digram (Example 2)

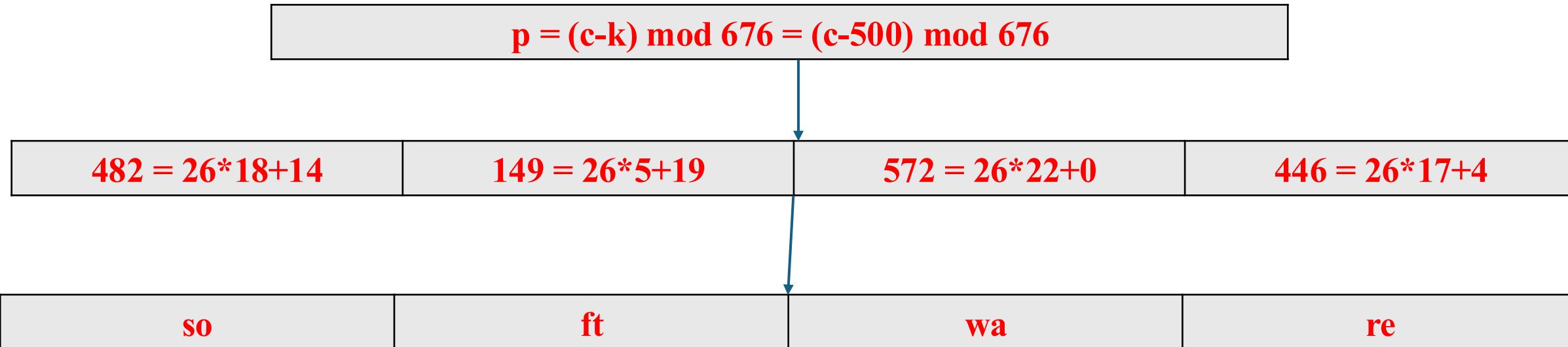
Decrypt the message “luyzpgkk” using key = 500, and additive cipher using digrams. Assume that the alphabets are case-insensitive and use the default numerical equivalents.

Solution:-

lu	yz	pg	kk
$26*11+20 = 306$	$26*24+25 = 649$	$26*15+6 = 396$	$26*10+10 = 270$



Additive Cipher with digram (Example 2) (Contd..)



- The decrypted text is “**software**”.

Caesar Cipher

- $c = (p+3) \bmod 26$
- $d = (c-3) \bmod 26$
- Ciphertext corresponding to the plaintext “udupi” is “xgxsl”
- Plaintext corresponding to the ciphertext “pdqlsdo” is “manipal”.
- However, Caesar cipher is generalized as additive cipher to use key of any value.

Pros and Cons of Additive Cipher

- Simple to understand, and Easy to implement.
- Demands negligible computational resources.

- Highly vulnerable to BFA.
- Vulnerable to Statistical attack.

HILL CIPHER

Hill Cipher

- Developed by Lester Hill in 1929.
- Uses concepts of Linear Algebra.
- $C = P * K \pmod{26}$, where P is of order $m*n$, and K is of order $n*n$.
- $D = C * K^{-1} \pmod{26}$
- Note:- K is an invertible matrix, and $\text{GCD}(\det(K), 26) = 1$

Example 1

- Encrypt the plaintext “**engineer**” using Hill Cipher with the key matrix displayed below. Assume that only alphabets are used for encryption/decryption, by ignoring the case.

$$K = \begin{bmatrix} 5 & 6 \\ 3 & 9 \end{bmatrix}$$

Solution:-

$$\bullet P = \begin{bmatrix} e & n \\ g & i \\ n & e \\ e & r \end{bmatrix} = \begin{bmatrix} 4 & 13 \\ 6 & 8 \\ 13 & 4 \\ 4 & 17 \end{bmatrix}$$

$$\bullet C = P * K \pmod{26}$$

Example 1 (Contd..)

$$\bullet C = \begin{bmatrix} 4 & 13 \\ 6 & 8 \\ 13 & 4 \\ 4 & 17 \end{bmatrix} * \begin{bmatrix} 5 & 6 \\ 3 & 9 \end{bmatrix} \pmod{26} = \begin{bmatrix} 59 & 141 \\ 54 & 108 \\ 77 & 114 \\ 71 & 177 \end{bmatrix} \pmod{26}$$

$$\bullet C = \begin{bmatrix} 7 & 11 \\ 2 & 4 \\ 25 & 10 \\ 19 & 21 \end{bmatrix} = \begin{bmatrix} h & i \\ c & e \\ z & k \\ t & v \end{bmatrix}$$

• Therefore, the ciphertext is “**hlcezk**tv”.

Example 2

- Decrypt the ciphertext “hlcezktv” using Hill Cipher with the key matrix displayed below. Assume that only alphabets are used for encryption/decryption, by ignoring the case.

$$K = \begin{bmatrix} 5 & 6 \\ 3 & 9 \end{bmatrix}$$

Solution:-

- $\det(K) = 27$

$$\bullet C = \begin{bmatrix} h & l \\ c & e \\ z & k \\ t & v \end{bmatrix} = \begin{bmatrix} 7 & 11 \\ 2 & 4 \\ 25 & 10 \\ 19 & 21 \end{bmatrix}$$

Example 2 (Contd..)

$$\bullet K^{-1} = \begin{bmatrix} 9 & -6 \\ -3 & 5 \end{bmatrix} * 27^{-1} \pmod{26}$$

q	a	b	r	u1	u2	u
1	27	26	1	1	0	1
26	26	1	0	0	1	-26
	1	0		1	-26	

$$\bullet K^{-1} = \begin{bmatrix} 9 & -6 \\ -3 & 5 \end{bmatrix} * 1 \pmod{26} = \begin{bmatrix} 9 & 20 \\ 23 & 5 \end{bmatrix}$$

Example 2 (Contd..)

- $D = C * K^{-1} \pmod{26} = \begin{bmatrix} 7 & 11 \\ 2 & 4 \\ 25 & 10 \\ 19 & 21 \end{bmatrix} * \begin{bmatrix} 9 & 20 \\ 23 & 5 \end{bmatrix} \pmod{26}$
- $D = \begin{bmatrix} 316 & 195 \\ 110 & 60 \\ 455 & 550 \\ 654 & 485 \end{bmatrix} \pmod{26} = \begin{bmatrix} 4 & 13 \\ 6 & 8 \\ 13 & 4 \\ 4 & 17 \end{bmatrix} = \begin{bmatrix} e & n \\ g & i \\ n & e \\ e & r \end{bmatrix}$
- Therefore, the decrypted text is “**engineer**”.

Example 3

- Decrypt the ciphertext “**rilmwbkaspdh**” using Hill Cipher with the key matrix displayed below. Assume that only alphabets are used for encryption/decryption, by ignoring the case.

$$K = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$$

Solution:-

$$C = \begin{bmatrix} r & r & l \\ m & w & b \\ k & a & s \\ p & d & h \end{bmatrix} = \begin{bmatrix} 17 & 17 & 11 \\ 12 & 22 & 1 \\ 10 & 0 & 18 \\ 15 & 3 & 7 \end{bmatrix}$$

Example 3 (Contd..)

$$\bullet K^{-1} = \begin{bmatrix} 300 & -313 & 267 \\ -357 & 313 & -252 \\ 6 & 0 & -51 \end{bmatrix} * (-939)^{-1} \pmod{26}$$

$$\bullet K^{-1} = \begin{bmatrix} -300 & 313 & -267 \\ 357 & -313 & 252 \\ -6 & 0 & 51 \end{bmatrix} * (939)^{-1} \pmod{26}$$

$$\bullet K^{-1} = \begin{bmatrix} -300 & 313 & -267 \\ 357 & -313 & 252 \\ -6 & 0 & 51 \end{bmatrix} * 9 \pmod{26} = \begin{bmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{bmatrix}$$

Example 3 (Contd..)

$$\bullet D = C * K^{-1} \pmod{26} = \begin{bmatrix} 17 & 17 & 11 \\ 12 & 22 & 1 \\ 10 & 0 & 18 \\ 15 & 3 & 7 \end{bmatrix} * \begin{bmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{bmatrix} \pmod{26}$$

$$\bullet D = \begin{bmatrix} 587 & 442 & 544 \\ 402 & 482 & 329 \\ 472 & 90 & 456 \\ 273 & 186 & 362 \end{bmatrix} \pmod{26} = \begin{bmatrix} 15 & 0 & 24 \\ 12 & 14 & 17 \\ 4 & 12 & 14 \\ 13 & 4 & 24 \end{bmatrix} = \begin{bmatrix} p & a & y \\ m & o & r \\ e & m & o \\ n & e & y \end{bmatrix}$$

- Therefore, the decrypted text is “**paymoremoney**”.

Pros and Cons of Hill Cipher

- Simple and Easy to understand and implement with prior knowledge of linear algebra.
 - More resistant to statistical attack than that for any other monoalphabetic ciphers.
 - Use of matrices adds an additional level of security.
-
- Limited key size and key space if 2×2 matrix is used as the key.
 - Poor efficiency for encrypting and decrypting data using large key matrices.

VIGENERE CIPHER

Vigenere Cipher

- The length of the key is made equal to that of the plaintext or ciphertext if its not the case already.
- $c_i = (p_i + k_i \text{ mod } m) \text{ mod } 26$
- $p_i = (c_i - k_i \text{ mod } m) \text{ mod } 26$
- Typically, m is lesser than the length of plaintext or ciphertext.

Example 1

- Encrypt the plaintext “**karnataka**” using Vigenere Cipher and the key “**hello**”. Assume that the encryption/decryption is done using only alphabets by ignoring the case.

Solution:-

PT	k (10)	a (0)	r (17)	n (13)	a (0)	t (19)	a (0)	k (10)	a (0)
-----------	-------------------------	------------------------	-------------------------	-------------------------	------------------------	-------------------------	------------------------	-------------------------	------------------------

+

Key	h (7)	e (4)	l (11)	l (11)	o (14)	h (7)	e (4)	l (11)	l (11)
------------	------------------------	------------------------	-------------------------	-------------------------	-------------------------	------------------------	------------------------	-------------------------	-------------------------

(mod 26) =

Example 1 (Contd..)

CT	17 (r)	4 (e)	2 (c)	24 (y)	14 (o)	0 (a)	4 (e)	21 (v)	11 (l)
-----------	-----------	----------	----------	-----------	-----------	----------	----------	-----------	-----------

- Therefore, the ciphertext is “**recyoaevl**”.

Example 2

- Decrypt the ciphertext “**recyoaevl**” using Vigenere Cipher and the key “**hello**”. Assume that the encryption/decryption is done using only alphabets by ignoring the case.

Solution:-

CT	r (17)	e (4)	c (2)	y (24)	o (14)	a (0)	e (4)	v (21)	I (11)
----	-----------	----------	----------	-----------	-----------	----------	----------	-----------	-----------

-

Key	h (7)	e (4)	I (11)	I (11)	o (14)	h (7)	e (4)	I (11)	I (11)
-----	----------	----------	-----------	-----------	-----------	----------	----------	-----------	-----------

$$(\text{mod } 26) =$$

Example 2 (Contd..)

PT	10 (k)	0 (a)	17 (r)	13 (n)	0 (a)	19 (t)	0 (a)	10 (k)	0 (a)
-----------	-----------	----------	-----------	-----------	----------	-----------	----------	-----------	----------

- Therefore, the decrypted text is “**karnataka**”.

Example 3

- Decrypt the ciphertext “yitpiyxugubnmtf” using Vigenere Cipher and the key “manipal”. Assume that the encryption/decryption is done using only alphabets by ignoring the case.

Solution:-

CT	y (24)	i (8)	t (19)	p (15)	i (8)	y (24)	x (23)	u (20)	g (6)	u (20)	b (1)	n (13)	m (12)	t (19)	f (5)
----	-----------	----------	-----------	-----------	----------	-----------	-----------	-----------	----------	-----------	----------	-----------	-----------	-----------	----------

-

Key	m (12)	a (0)	n (13)	i (8)	p (15)	a (0)	l (11)	m (12)	a (0)	n (13)	i (8)	p (15)	a (0)	l (11)	m (12)
-----	-----------	----------	-----------	----------	-----------	----------	-----------	-----------	----------	-----------	----------	-----------	----------	-----------	-----------

$\pmod{26} =$

Example 3 (Contd..)

PT	12 (m)	8 (i)	6 (g)	7 (h)	19 (t)	24 (y)	12 (m)	8 (i)	6 (g)	7 (h)	19 (t)	24 (y)	12 (m)	8 (i)	19 (t)
----	-----------	----------	----------	----------	-----------	-----------	-----------	----------	----------	----------	-----------	-----------	-----------	----------	-----------

- Therefore, the decrypted text is “mightymightymit”.

Pros and Cons of Vigenere Cipher

- Simple to understand and easy to implement.
 - More resistant to statistical attack and pattern attack when compared to that of monoalphabetic ciphers.
 - When the PT is long, the cipher is resistant to BFA if the key is long enough.
-
- Vulnerable to BFA if PT is extremely short.
 - Vulnerable to statistical attack if key length is significantly lesser than that of the plaintext.
 - Vulnerable to pattern attack if key length is significantly lesser than that of the plaintext.

PLAYFAIR CIPHER

Playfair Cipher

- Invented by Charles Wheatstone in the year 1854.
- Encrypts or decrypts digrams.
- Key is a 5×5 matrix with all the alphabets (letters i and j are considered as a single entry appropriately) arranged row-wise.

Generation of key matrix from key

- Initially the alphabets of the key are arranged row-wise in a 5*5 matrix, by removing duplicates from the key.
- Rest of the vacancies of the matrix are filled with remaining alphabets.

Generation of key matrix from key (Example 1)

- Consider that the key is “UDUPI”.
- The corresponding key matrix will be:-

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

Generation of key matrix from key (Example 2)

- Consider that the key is “JAIPUR”.
- The corresponding key matrix will be:-

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

Steps for Processing Plaintexts

- Plaintext is processed as each digram at a time.
- Plaintext is modified (if necessary) to make sure that no digram has a duplicate alphabet (by replacing a duplicate alphabet by x).
- Plaintext is modified (if necessary) to make sure that no alphabet is left unpaired (by adding x to the last alphabet of the original plaintext to make it form a digraph).
- **FEVER → FEVERX**
- **SHEEP → SHEXEP**
- **TEAM → TEAM**

Steps for Encrypting a Plaintext

- If both the alphabets of a digram are in the same row, then each alphabet is replaced by the alphabet immediately towards its right, in the row by considering right rotation.
- If both the alphabets of a digram are in the same column, then each alphabet is replaced by the alphabet immediately below it in the column by considering top-bottom rotation.
- Else, in a digram each alphabet is replaced by the alphabet which is in the same row but in the column of the other alphabet of the digraph.

Steps for Decrypting a Ciphertext

- If both the alphabets of a digram are in the same row, then each alphabet is replaced by the alphabet immediately towards its left, in the row by considering left rotation.
- If both the alphabets of a digram are in the same column, then each alphabet is replaced by the alphabet immediately above it in the column by considering bottom-top rotation.
- Else, in a digraph each alphabet is replaced by the alphabet which is in the same row but in the column of the other alphabet of the digram.

Example 1

- Encrypt the plaintext “CHENNAI” using the key “MANGALORE”.

Solution:-

- Key matrix:-

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

- Modified PT = CHENNAIX

Example 1 (Contd..)

- CH → EK
- EN → HE
- NA → GN
- IX → HY
- Therefore, the ciphertext is “EKHEGNHY”.

Example 2

- Decrypt the ciphertext “EKHEGNHY” using the key “MANGALORE”.

Solution:-

- Key matrix:-

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

- Modified CT = EKHEGNHY

Example 2 (Contd..)

- EK → CH
 - HE → EN
 - GN → NA
 - HY → IX
-
- The decrypted text is “**CHEENNAIX**”.
 - Therefore, the final decrypted text is “**CHEENNAI**”.

Example 3

- Encrypt the plaintext “HELLOINDIA” using the key “PLAYFAIR”.

Solution:-

- Key matrix:-

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

- Modified PT = HELXLOINDIAX

Example 3 (Contd..)

- HE → KG
 - LX → YV
 - LO → RV
 - IN → EU
 - DI → IR
 - AX → YW
-
- Therefore, the ciphertext is “KGYVRVEUIR”.

Example 4

- Decrypt the ciphertext “LGXNDODENPDSAU” using the key “PRINCIPLESOFCRYPTOGRAPHY”.

Solution:-

- Key matrix:-

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

- Modified CT = LGXNDODENPDSAU

Example 4 (Contd..)

- LG → SY
 - XN → MX
 - DO → ME
 - DE → TR
 - NP → IC
 - DS → KE
 - AU → YX
-
- The decrypted text is “SYMXXMETRICKEYX”.
 - Therefore, the final decrypted text is “SYMMETRICKEY”.

Story time

1. BSSBKQBSFRSW, key: History
2. BINBZTNBKNDMQDRW, key: Dawn
3. IDXWQFBSMXBQZOGQWEFCIZQG , key : Dawn

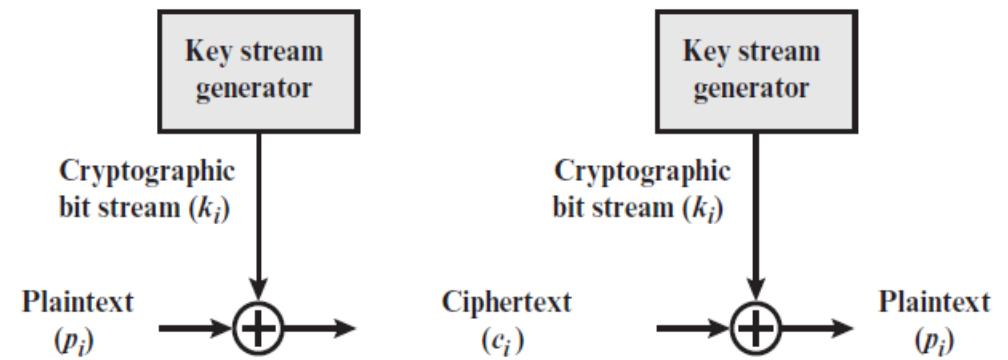
Pros and Cons of Playfair Cipher

- Simple to understand and easy to implement when the plaintext length is even and when the original digrams don't have duplicate alphabets.
 - BFA on the cipher is almost impossible.
 - Resistant to statistical and pattern attacks when the plaintexts are short.
 - Key Management is easy.
-
- Implementation gets complicated when the plaintext length is odd, or the original digrams have duplicate alphabets.
 - Vulnerable to statistical and pattern attacks when the plaintexts are long (> 1000 characters).

VERNAM CIPHER

Vernam Cipher

- Introduced by Gilbert Vernam in 1918.
- Length of the plaintext = Length of the key.
- More resistant to statistical attack when compared to Vigenere cipher.
- Initially, the algorithm was proposed with repeating phrases in the key.



One Time Pad

- Improved version of Vernam Cipher.
- Length of the key (random) = Length of the plaintext
- The key is discarded after every session.
- Produces a random ciphertext.
- Statistical attack becomes almost impossible.

One Time Pad (Examples)

- Encryption of “**cryptography**” using the key “**zabbcgvikjyx**” is “**brzqvubzkyfv**” (using only alphabets by ignoring the case).
- Encryption of “**cryptography**” using the key “**aghhqztuypfr**” is “**cxfwjnzlyemp**” (using only alphabets by ignoring the case).
- Encryption of “**operatingsystems**” using the key “**xgpuukrxfeprsrxal**” is “**lvtludzklwnkkbmd**” (using only alphabets by ignoring the case).

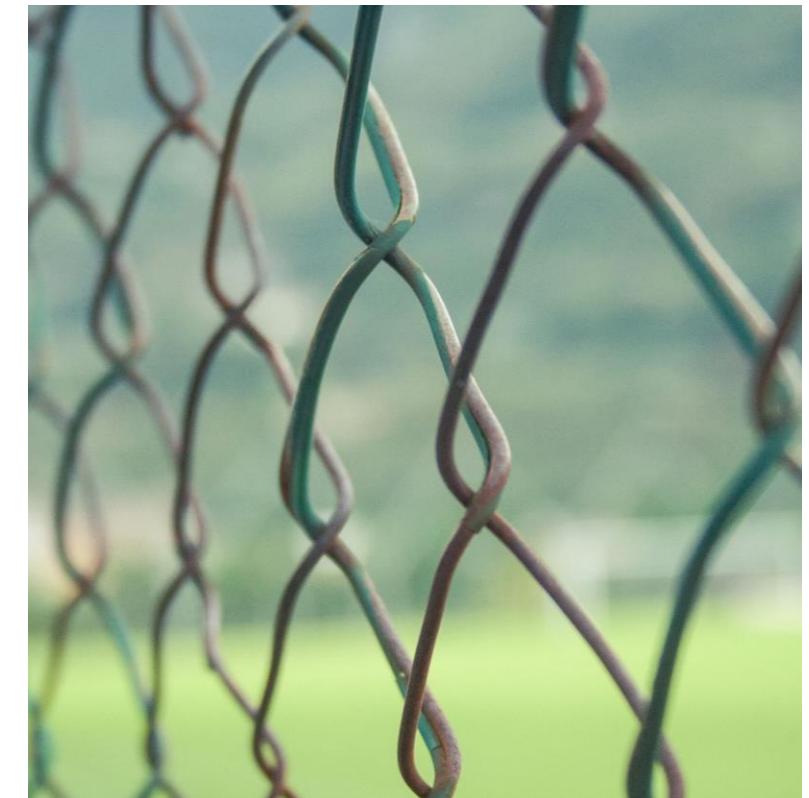
Disadvantages of using One Time Pad

- Generation of large random key for every session, when the plaintext is huge.
- Key Management becomes harder.
- Most probably its used for only low bandwidth channels.

RAIL FENCE CIPHER

Rail Fence Cipher

- Encryption:- The plaintext characters are written as a sequence of diagonals in a table based on the depth (Number of rows = depth) in a zig-zag manner. The ciphertext is obtained by reading the characters in the Rail Fence table, row-wise.
- Decryption:- Create a blank table with rows equal to the depth and columns equal to the length of the ciphertext. Enter the first ciphertext character in the top-left cell, then move diagonally down to the last row and back up to the first row, placing the next character in the corresponding column when you return to the top. Continue this process, leaving blank spaces as needed until all characters are placed. Fill any remaining blank spaces row-wise with the remaining ciphertext characters. To decrypt, read the ciphertext characters diagonally in a zig-zag pattern.



Example 1

- Encrypt the plaintext “KANNIYAKUMARI” using Rail fence cipher with a depth of 2.

Solution:-

K		N		I		A		U		A		I
	A		N		Y		K		M		R	

- The ciphertext is “KNIAUAIAKYKMR”.

Example 2 (Contd..)

- Iteration 2:-

K		N		I		A		U		A		I
	A		N		Y		K		M		R	

- Therefore, the decrypted text is “KANNIYAKUMARI”.

Example 3

- Encrypt the plaintext “COMPUTERNETWORKS” using Rail Fence cipher with a depth of 3.

Solution:-

C				U			N			O				
	O		P	T		R	E		W		R			S
		M			E			T			K			

- The ciphertext is “CUNOOPTREWRSMETK”.

Example 4

- Decrypt the ciphertext “CUNOOPTREWRSMETK” using Rail fence cipher with a depth of 3.

Solution:-

- Iteration 1:-

C					U				N				O			
	—		—		—		—		—		—		—		—	
		—				—				—			—			—

Example 4 (Contd..)

- Iteration 2:-

C				U			N			O				
	O		P		T		R		E		W		R	S
		M				E				T			K	

- Therefore, the decrypted text is “COMPUTERNETWORKS”.

Example 5

- Decrypt the ciphertext “MLRAAAUESNPNVIIIT” using Rail fence cipher with a depth of 4.

Solution:-

- Iteration 1:-

M					L					R					
	—				—					—					
		—		—				—			—		—		
			—						—				—		

Example 5 (Contd..)

- Iteration 2:-

M					L					R							
	A				A		U			E		S					
	N		P			N		V			I		Y				
		I						I				T					

- The decrypted text is “MANIPALUNIVERSITY”.

Pros and Cons of Rail Fence Cipher

- Simple to understand and easy to implement.
- Has got low computation cost.

- Vulnerable to Statistical attack.
- Vulnerable to Pattern attack.
- Vulnerable to BFA.

COLUMNAR CIPHER

Columnar Cipher

- Provides grid-based encryption and decryption.
- The plaintext is written row-wise, and the ciphertext is generated by reading the plaintext characters column-wise.
- The ciphertext is written column-wise in a certain order, and the decrypted text is generated by reading the ciphertext characters row-wise.
- The key contains a sequence of numbers representing the order of columns.
- Multiple stages can be used to enhance the security.



Processing the key

- The key could either be represented as a sequence of numbers or as a text.
- If the key is a text, then the text is converted into a sequence of numbers according their alphabetical order in the text.
- The length of the key = number of columns.
- Assume that the key is ‘4 2 1 3 5’. This indicates that the grid consists of 5 columns.
- If the key is ‘hello’, then the corresponding sequence of numbers for the key would be ‘2 1 3 4 5’.



Steps for Encryption

- Number of Rows = $\text{Ceil}(\text{Length(PT)}/\text{Number of Columns})$
- Fill the grid row-wise with plaintext characters (At the end, fill any vacancy with ‘x’).
- Obtain the ciphertext, by reading the plaintext characters column-wise according to sequence of numbers.
- For example, a key having a sequence ‘3 1 2’ indicates that the grid has 3 columns. Moreover, during CT calculation, the second column is read first, third column is read second, and the first column is read third.



Steps for Decryption

- Number of Rows = Length(CT)/Number of Columns
- Fill the grid column-wise with the Ciphertext characters according to sequence of numbers in the key.
- Obtain the Plaintext by reading the Ciphertext characters row-wise.
- For example, if the key has a sequence ‘3 1 2’, then the second column is filled first, third column is filled second, and the first column is filled third.



Example 1

- Encrypt the plaintext “GOCORONAGO” using single stage columnar transposition with key “HELLO”.

Solution:-

- “HELLO” → “2 1 3 4 5”

G	O	C	O	R
O	N	A	G	O

- Therefore, the Ciphertext is “ONGOCAOGRO”.

Example 2

- Decrypt the Ciphertext “ONGOCAGOOGRO” using single stage columnar transposition with key “HELLO”.

Solution:-

- “HELLO” → “2 1 3 4 5”
- IT1:-

	O			
	N			

Example 2 (Contd..)

- IT2:-

G	O			
O	N			

- IT3:-

G	O	C	O	R
O	N	A	G	O

- Therefore, the decrypted text is “GOCORONAGO”.

Example 3

- Encrypt the plaintext “GOCORONAGO” using double stage columnar transposition with key “HELLO”.

Solution:-

- “HELLO” → “2 1 3 4 5”

G	O	C	O	R
O	N	A	G	O

- CT after first stage encryption:- “ONGOCAOGRO”.

Example 3 (Contd..)

- Now encrypt “ONGOCAOOGRO”.

2	1	3	4	5
O	N	G	O	C
A	O	G	R	O

- Therefore, the final Ciphertext is “NOOAGGORCO”.

Example 4

- Decrypt the Ciphertext “NOOAGGORCO” using double stage columnar transposition with key “HELLO”.

Solution:-

- “HELLO” → “2 1 3 4 5”

O	N	G	O	C
A	O	G	R	O

- Decrypted text after first stage decryption:- “ONGOCAOGRO”.

Example 4 (Contd..)

- Now decrypt “ONGOCAOOGRO” again.

2	1	3	4	5
G	O	C	O	R
O	N	A	G	O

- Hence, the final decrypted text is “GOCORONAGO”.

Example 5

- Decrypt the Ciphertext “CALONAIIXACEIEIEMUMHXAHXADFXYRPODTNG” using double stage columnar transposition with key “MANIPAL”.

Solution:-

- “MANIPAL” →

5	1	6	3	7	2	4
---	---	---	---	---	---	---

Example 5 (Contd..)

5	1	6	3	7	2	4
---	---	---	---	---	---	---

A	C	F	E	O	A	M
H	A	X	I	D	I	U
X	L	Y	E	T	X	M
A	O	R	I	N	A	H
D	N	P	E	G	C	X

- The decrypted text after first stage decryption:-
“ACFEOAMHAXIDIUXLYETXMAORINAHDNPEGCX”.

Example 5 (Contd..)

- Now decrypt “ACFEOAMHAXIDIUXLYETXMAORINAHDNPEGCX” again.

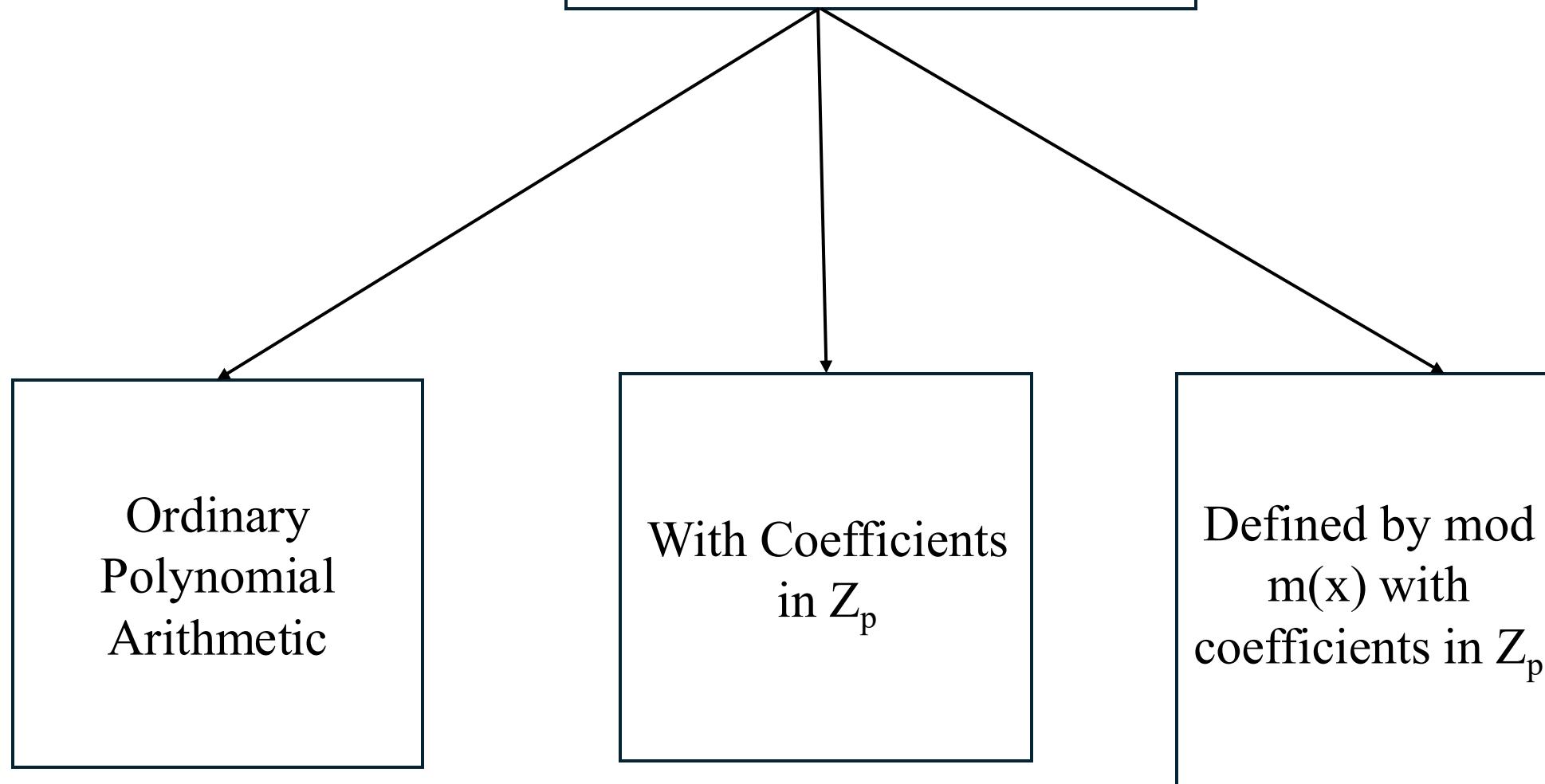
5	1	6	3	7	2	4
M	A	N	I	P	A	L
A	C	A	D	E	M	Y
O	F	H	I	G	H	E
R	E	D	U	C	A	T
I	O	N	X	X	X	X

- The decrypted text after second stage decryption:-
“MANIPALACADEMYOFHIGHREDUCATIONXXXX”.
- Hence, truncating the 4 ‘X’s at the end, the decrypted text is
“MANIPALACADEMYOFHIGHREDUCATION”.

Pros and Cons of Columnar Transposition Cipher

- Simple to understand and straight forward to implement for short texts.
 - Efficient for short texts.
 - At times more resistant to statistical attack when compared to substitution attack.
-
- Highly vulnerable to Pattern analysis attack, when a short key is used, with a single stage transposition.
 - Decrypting long ciphertexts could produce errors, if not implemented properly.

Polynomial Arithmetic



ORDINARY POLYNOMIAL ARITHMETIC

Ordinary Polynomial Arithmetic

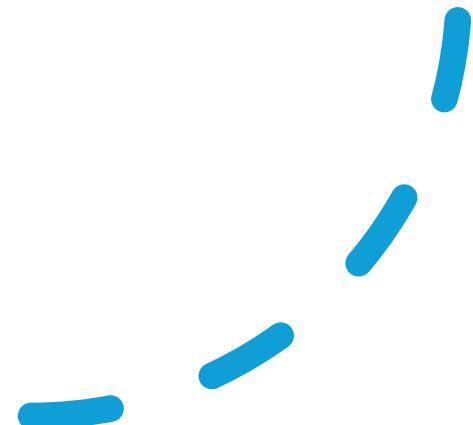
A **polynomial** of degree n (integer $n \geq 0$) is an expression of the form

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = \sum_{i=0}^n a_i x^i$$

where the a_i are elements of some designated set of numbers S , called the **coefficient set**, and $a_n \neq 0$. We say that such polynomials are defined over the coefficient set S .

Ordinary Polynomial Arithmetic

- Zero Degree Polynomial (when $n = 0$)
- Monic Polynomial (when $a_n = 1$)
- In Abstract Algebra, x is also called as indeterminate.



Ordinary Polynomial Arithmetic

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

(a) Addition

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

(b) Subtraction

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

(c) Multiplication

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

(d) Division

Modular Polynomial Arithmetic

- $r(x) = f(x) \bmod g(x)$
- When $f(x) = x^3 + x^2 + 2$ and $g(x) = x^2 - x + 1$, $r(x) = x$
- When $f(x) = x^7 + x^5 + x^4 + x^3 + x + 1$ and $g(x) = x^3 + x + 1$, $r(x) = 0$

Polynomials in GF(p)

GF(2)

- Polynomial Addition and Subtraction are the same.
- Polynomial Addition is equivalent to XOR operation.
- Polynomial Multiplication is equivalent to Logical AND operation.

GF(2) (Example 1)

- $f(x) = x^6 + x^5 + x^2 + 1$
- $g(x) = x^3 + x^2 + 1$
- In GF(2), $f(x) + g(x) = ?$

Solution:-

- $f(x) + g(x) = x^6 + x^5 + x^3$

GF(2) (Example 2)

- $f(x) = x^6 + x^3 + x^2 + 1$
- $g(x) = x^6 + x^5 + x^3 + x + 1$
- In GF(2), $f(x) + g(x) = ?$

Solution:-

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

GF(2) (Example 3)

- $f(x) = x^6 + x^3 + x^2 + 1$
- $g(x) = x^6 + x^5 + x^3 + x + 1$
- In GF(2), $f(x) * g(x) = ?$

Solution:-

- $f(x) * g(x) = x^6 * (x^6 + x^5 + x^3 + x + 1) + x^3 * (x^6 + x^5 + x^3 + x + 1) + x^2 * (x^6 + x^5 + x^3 + x + 1) + (x^6 + x^5 + x^3 + x + 1)$
- $f(x) * g(x) = x^{12} + x^{11} + x^6 + x^4 + x^3 + x^2 + x + 1$

GF(2) (Example 4)

- $f(x) = x^3 + x^2 + x + 1$
- In GF(2), $[f(x)]^2 = ?$

Solution:-

- $[f(x)]^2 = x^6 + x^4 + x^2 + 1$

GF(2) (Example 5)

- $f(x) = x^6 + x^5 + x^2 + x + 1$
- $g(x) = x^3 + x^2 + 1$
- In GF(2), $f(x)/g(x) = ?$, $f(x) \bmod g(x) = ?$

Solution:-

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

GF(2) (Example 6)

- $f(x) = x^7 + x^6 + x^5 + x^2 + 1$
- $g(x) = x^3 + x^2 + x + 1$
- In GF(2), $f(x)/g(x) = ?$, $f(x) \bmod g(x) = ?$

Solution:-

- $f(x)/g(x) = x^4 + x + 1$
- $f(x) \bmod g(x) = x^2$

GF(2) (Example 7)

- $f(x) = x^4 + x^3 + x^2 + x$
- $g(x) = x^2 + 1$
- In GF(2), $f(x)/g(x) = ?$, $f(x) \bmod g(x) = ?$

Solution:-

- $f(x)/g(x) = x^2 + x$
- $f(x) \bmod g(x) = 0$

Irreducible Polynomials in GF(2)

- $f(x)$ is irreducible if it can't be expressed as a product of any 2 non-constant polynomials of lower degrees.
- Also called as Prime polynomials.

Degree	Irreducible Polynomials
1	$x, (x+1)$
2	$x^2 + x + 1$
3	$(x^3 + x + 1), (x^3 + x^2 + 1)$
4	$(x^4 + x + 1), (x^4 + x^3 + 1), (x^4 + x^3 + x^2 + x + 1)$
5	$(x^5 + x^2 + 1), (x^5 + x^3 + 1), (x^5 + x^3 + x^2 + x + 1), (x^5 + x^4 + x^3 + x + 1), (x^5 + x^4 + x^2 + x + 1), (x^5 + x^4 + x^3 + x^2 + 1)$

Pseudocode for $\text{GCD}(f(x), g(x))$

```
GCD {f(x),g(x)}  
{  
if(g(x)==0)  
    return f(x);  
else  
    return GCD{g(x), f(x) mod g(x)}  
}
```

GCD (Example 1)

- $f(x) = x^6 + x^5 + x^4 + x^2 + x + 1$
- $g(x) = x^4 + x + 1$
- $\text{GCD}\{f(x), g(x)\} = ?$

Solution:-

$$\text{GCD}\{f(x), g(x)\} = \text{GCD}\{g(x), f(x) \bmod g(x)\} =$$

$$\text{GCD}\{(x^4 + x + 1), (x^6 + x^5 + x^4 + x^2 + x + 1) \bmod (x^4 + x + 1)\} =$$

$$\text{GCD}\{(x^4 + x + 1), (x^3 + x^2 + x)\} =$$

$$\text{GCD}\{(x^3 + x^2 + x), (x^4 + x + 1) \bmod (x^3 + x^2 + x)\} =$$

$$\text{GCD}\{(x^3 + x^2 + x), 1\} =$$

$$\text{GCD}\{1, (x^3 + x^2 + x) \bmod 1\} =$$

$$\text{GCD}(1, 0) = 1$$

Polynomials in $GF(p^m)$

- $f(x) = a_m x^m + a_{m-1} x^{m-1} + \dots + a_1 x + a_0$, where all the coefficients belong to $GF(p)$.
- All the operations are performed modulo any irreducible polynomial ($m(x)$) with degree m .
- For example, for Polynomial arithmetic over $GF(2^8)$, the coefficients are binary values, and a potential irreducible polynomial would be $(x^8 + x^4 + x^3 + x + 1)$.

Polynomial Arithmetic (Example 1)

- $f(x) = x^4 + x^3 + x^2 + x + 1$
- $g(x) = x^2 + 1$
- $m(x) = x^4 + x + 1$
- $f(x) + g(x) = ?$

Solution:-

- $[f(x) + g(x)] \text{ mod } m(x) = [(x^4 + x^3 + x^2 + x + 1) + (x^2 + 1)] \text{ mod } (x^4 + x + 1)$
- $[f(x) + g(x)] \text{ mod } m(x) = (x^4 + x^3 + x) \text{ mod } (x^4 + x + 1)$
- $[f(x) + g(x)] \text{ mod } m(x) = x^3 + 1$

Polynomial Arithmetic (Example 2)

- $f(x) = x^5 + x^4 + x^2 + x + 1$
- $g(x) = x^5 + x^4 + x^3 + x^2 + x + 1$
- $m(x) = x^8 + x^4 + x^3 + x + 1$
- $f(x) * g(x) = ?$

Solution:-

- $[f(x) * g(x)] \bmod m(x) = [(x^5 + x^4 + x^2 + x + 1) * (x^5 + x^4 + x^3 + x^2 + x + 1)] \bmod (x^8 + x^4 + x^3 + x + 1)$
- $[f(x) * g(x)] \bmod m(x) = (x^{10} + x^7 + x^5 + x^3 + x^2 + 1) \bmod (x^8 + x^4 + x^3 + x + 1)$
- $[f(x) * g(x)] \bmod m(x) = x^7 + x^6 + 1$

Polynomial Arithmetic (Example 3)

- $f(x) = x^4 + x + 1$
- $g(x) = x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + 1$
- $m(x) = x^6 + x^5 + x^4 + x + 1$
- $f(x) * g(x) = ?$

Solution:-

- $[f(x) * g(x)] \bmod m(x) = [(x^4 + x + 1) * (x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + 1)] \bmod (x^6 + x^5 + x^4 + x + 1)$
- $[f(x) * g(x)] \bmod m(x) = (x^{11} + x^{10} + x^9 + x^7 + x^6 + x^4 + x^2 + x + 1) \bmod (x^6 + x^5 + x^4 + x + 1)$
- $[f(x) * g(x)] \bmod m(x) = x^5 + x$

Extended Euclidean Algorithm (EEA) on Polynomials in $GF(p)$ and $GF(p^m)$

Pseudocode for EEA

```
EEA {a(x), b(x)}
```

```
{
```

```
    u1(x)=1, u2(x)=0, v1(x)=0, v2(x)=1;
```

```
    while(b(x)≠0)
```

```
{
```

```
        q(x)=a(x)/b(x); r(x)=a(x) mod b(x); u(x)=u1(x)-q(x)*u2(x); v=v1(x)-q(x)*v2(x);  
        a(x)=b(x); b(x)=r(x); u1(x)=u2(x); u2(x)=u(x); v1(x)=v2(x); v2(x)=v(x);
```

```
}
```

```
    return(a(x), u1(x), v1(x))
```

```
}
```

EEA (Example 1)

- $a(x) = x^3 + x + 1$
- $b(x) = x^2 + 1$
- Calculate $\text{GCD}\{a(x), b(x)\} = a(x)*u_1(x) + b(x)*v_1(x)$, and calculate $u_1(x)$ and $v_1(x)$, in $\text{GF}(2)$

Solution:-

Iteration 1:-

$a(x) = x^3 + x + 1$; $b(x) = x^2 + 1$; $q(x) = x$; $r(x) = 1$; $u_1(x) = 1$; $u_2(x) = 0$; $u(x) = 1$; $v_1(x) = 0$; $v_2(x) = 1$, $v(x) = x$

EEA (Example 1) (Contd..)

Iteration 2:-

$$a(x) = x^2 + 1, b(x) = 1; q(x) = x^2 + 1; r(x) = 0; u_1(x) = 0; u_2(x) = 1; u(x) = x^2 + 1;$$
$$v_1(x) = 1; v_2(x) = x, v(x) = x^3 + x + 1$$

Iteration 3:-

$$a(x) = 1; b(x) = 0; u_1(x) = 1, u_2(x) = x^2 + 1, v_1(x) = x, v_2(x) = x^3 + x + 1$$

- Therefore $\text{GCD}\{(a(x), b(x)\} = 1; u_1(x) = 1; v_1(x) = x;$
- Also, we can say that $\text{MI}(x^3 + x + 1) \bmod (x^2 + 1) = 1$

EEA (Example 2)

- Calculate MI(x^2+1) mod ($x^4 + x + 1$) in GF(2^4)

Solution:-

Iteration 1:-

$$a(x) = x^4 + x + 1; b(x) = x^2 + 1; q(x) = x^2 + 1; r(x) = x;$$

$$v1(x) = 0; v2(x) = 1; v(x) = x^2 + 1$$

Iteration 2:-

$$a(x) = x^2 + 1; b(x) = x; q(x) = x; r(x) = 1;$$

$$v1(x) = 1; v2(x) = x^2 + 1; v(x) = x^3 + x + 1$$

EEA (Example 2) (Contd..)

Iteration 3:-

$$a(x) = x; b(x) = 1; q(x) = x; r(x) = 0;$$

$$v1(x) = x^2 + 1; v2(x) = x^3 + x + 1; v(x) = (x^4 + x + 1) \bmod (x^2 + 1) = 0$$

Iteration 4:-

$$a(x) = 1; b(x) = 0;$$

$$v1(x) = x^3 + x + 1; v2(x) = 0$$

- Therefore, $MI(x^2+1) \bmod (x^4 + x + 1) = (x^3 + x + 1)$

EEA (Example 3)

- Calculate MI($x^4 + x^3 + x^2 + 1$) mod ($x^8 + x^4 + x^3 + x + 1$)

Solution:-

Iteration 1:-

$$a(x) = x^8 + x^4 + x^3 + x + 1; b(x) = x^4 + x^3 + x^2 + 1;$$

$$q(x) = x^4 + x^3 + x + 1; r(x) = x^2;$$

$$v1(x) = 0; v2(x) = 1; v(x) = x^4 + x^3 + x + 1$$

Iteration 2:-

$$a(x) = x^4 + x^3 + x^2 + 1; b(x) = x^2; q(x) = x^2 + x + 1; r(x) = 1;$$

$$v1(x) = 1; v2(x) = x^4 + x^3 + x + 1; v(x) = x^6$$

EEA (Example 3) (Contd..)

Iteration 3:-

$$a(x) = x^2; b(x) = 1; q(x) = x^2; r(x) = 0;$$

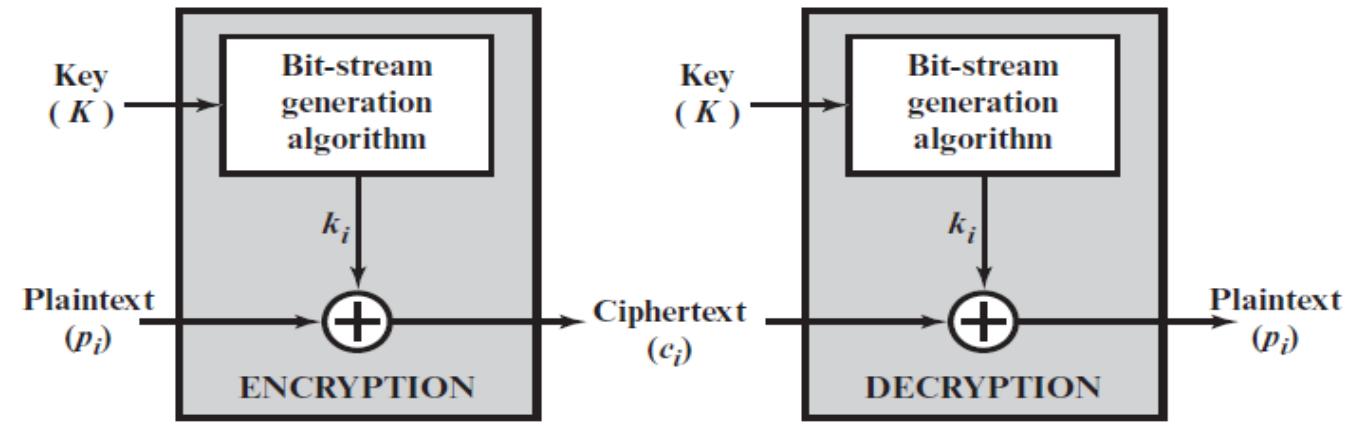
$$v1(x) = x^4 + x^3 + x + 1; v2(x) = x^6; v(x) = 0;$$

Iteration 4:-

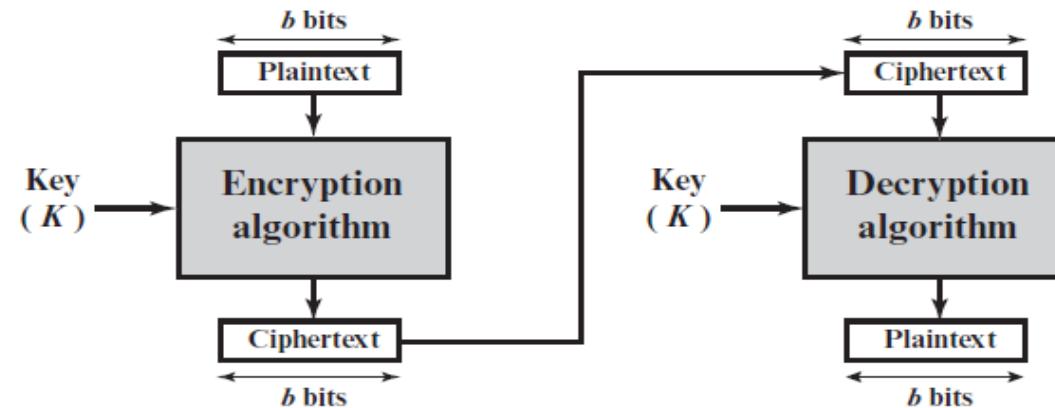
$$a(x) = 1; b(x) = 0; v1(x) = x^6; v2(x) = 0;$$

- Therefore, $MI(x^4 + x^3 + x^2 + 1) \text{ mod } (x^8 + x^4 + x^3 + x + 1) = x^6$

Stream Cipher and Block Cipher



(a) Stream cipher using algorithmic bit-stream generator



(b) Block cipher

Differences between Stream and Block Ciphers

Stream	Block
One Bit or Byte is processed (encrypted or decrypted) at a time	Fixed size block is processed at a time (64 bits, 128 bits, etc.)
Usually Variable Key size	A given algorithm will have a fixed key size
Padding is not required	Most probably requires padding
Processing is faster	Processing is slower
Error Propagation is limited	Error propagation could be significant and can produce a completely different output
Examples:- RC4, Rabbit, ChaCha, etc.	Examples:- AES, DES, Triple DES, Serpent, etc.
Used for real-time data stream encryptions and decryptions, where minimum latency is expected.	Used for applications which can handle large data chunks.

MOTIVATION FOR FEISTEL CIPHER STRUCTURE

n-bit to n-bit Block Substitution

- Block Cipher (n-bit PT block  n-bit CT block, and vice-versa)
- Number of PT blocks possible = 2^n .
- Decryption is possible when each PT block can produce a unique CT block (Reversible or Non-Singular Transformation).
- Reversible set of Transformations when $n = 2$:-

PT Block	CT Block
00	11
01	10
10	00
11	01

n-bit to n-bit Block Substitution (Contd..)

- Irreversible set of Transformations when $n = 2$:-

PT Block	CT Block
00	11
01	10
10	01
11	01

- Number of Reversible sets of transformations = $2^n!$

4-bit to 4-bit Block Substitution Example

Plaintext	Ciphertext
0000	1110
0001	0100
0010	1101
0011	0001
0100	0010
0101	1111
0110	1011
0111	1000
1000	0011
1001	1010
1010	0110
1011	1100
1100	0101
1101	1001
1110	0000
1111	0111

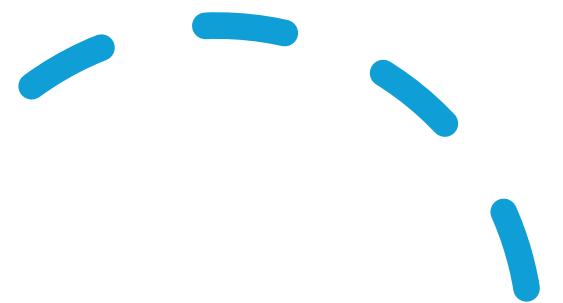
Ciphertext	Plaintext
0000	1110
0001	0011
0010	0100
0011	1000
0100	0001
0101	1100
0110	1010
0111	1111
1000	0111
1001	1101
1010	1001
1011	0110
1100	1011
1101	0010
1110	0000
1111	0101

n-bit to n-bit Block Substitutions (Contd..)

- We noticed with $n=2$, and $n=4$, that the corresponding tables define straightforward mappings between PT blocks and CT blocks.
- Feistel called these types of mappings as an ideal block cipher.
- Increasing the block size makes the block cipher more resistant to cryptanalysis.
- The mappings can be defined by a key whose length is $n*2^n$ bits.
- However, when n is huge, Key-Management becomes cumbersome.

BLOCK CIPHER DESIGN PRINCIPLES

Principles of designing a Block Cipher

- 
- 1) Confusion
 - 2) Diffusion
 - 3) Avalanche Effect
 - 4) Feistel Structure
 - 5) Round Functions
 - 6) Key Size and Block Size
 - 7) Bit Independence Criterion (BIC)
 - 8) Key Schedule Algorithm

Confusion

- Term was introduced by Claude Shannon.
- The property makes the relationship between the CT and the key as complex as possible.
- Achieved through Complex Key-Schedule and Substitution.
- Each bit of the CT depends on several bits of the key.

Diffusion

- The term was introduced by Claude Shannon.
- The property makes the relationship between the CT and PT complex.
- Achieved through mixing operations and Permutation.
- One bit change in the PT will result in significant change in the bits of CT.

Avalanche Effect

- Property which ensures that a small change in any of the Inputs results in a significant and unpredictable change in the Output.
- Achieved through Confusion and Diffusion.

Feistel Structure

- Used to achieve Confusion and Diffusion in an organized manner.
- Involves division of each block, operations through multiple rounds, and swapping operations.

Round Functions

- Internal functions used for each round of a Cipher.
- The functions are complex and foundations for Avalanche Effect.
- Involves Substitutions, Permutations, and Mixing Operations.

Key Size and Block Size

- Plays a crucial role in security.
- Larger the key, more is the Cipher resistant to BFA.
- Larger the PT block, more is the Cipher resistant to Statistical and Pattern attack.

BIC

- More associated with cryptographic hash functions and PRNGs.
- However, applicable to Block Cipher design as well.
- Provides statistically random output.
- Provides negligible or 0 predictable relationships between the current and the neighboring bits.

Key Schedule Algorithm

- Round keys are derived from a Master Key.
- Crucial Component in many block ciphers like DES, AES, etc.
- A good algorithm should generate unique and random round keys.
- Generated using different operations like Substitutions, Permutations, Mixing, Bit shifting operations, etc.

FEISTEL CIPHER

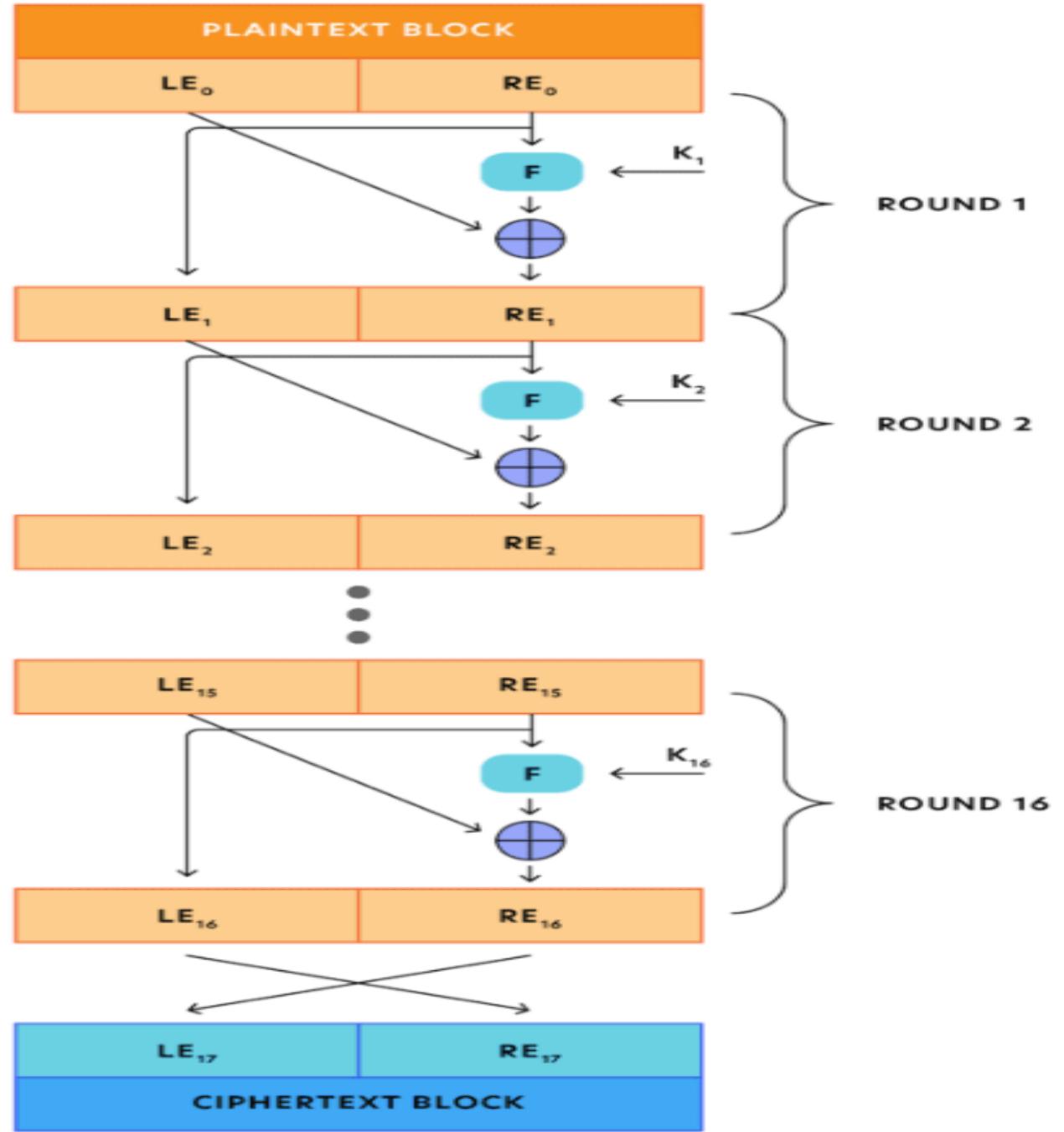
Feistel Cipher

- Key Length = k bits
- Number of sets of Transformations = 2^k
- Alternates Substitution and Permutation operations.
- Can have any number of rounds with same structure.

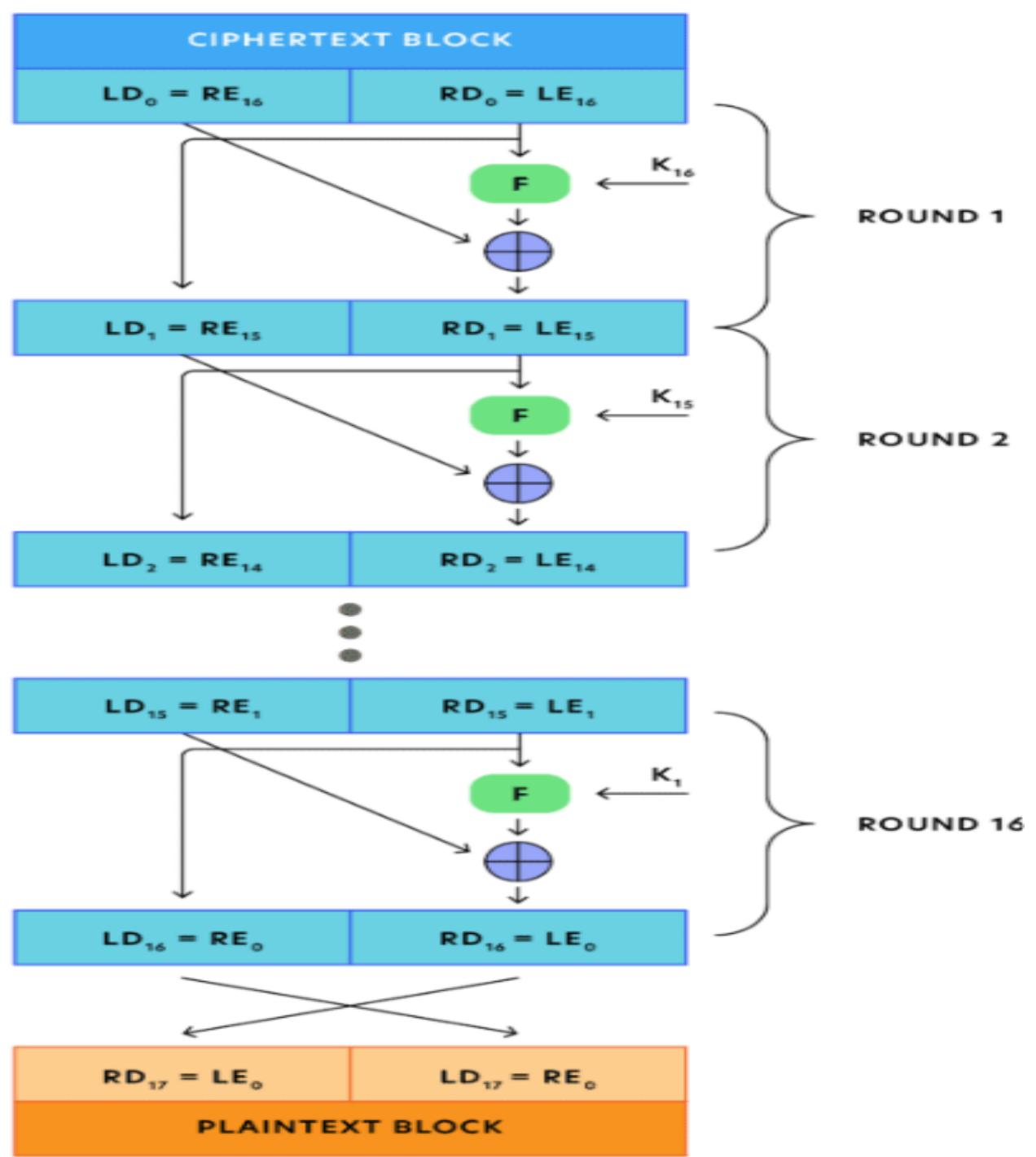
Design Features to be considered in Feistel Cipher

- Block size
- Ease of Analysis
- Key Size
- Sub-Keys generation Function
- Number of Rounds
- Round Function
- Fast software encryption/decryption

Encryption



Decryption



Observations in Encryption and Decryption

- Assume that n is the number of rounds.
- During Encryption, $LE_i = RE_{i-1}$
- During Encryption, $RE_i = LE_{i-1} \oplus F(RE_{i-1}, K_i)$
- During Decryption, $LD_i = RD_{i-1}$
- During Decryption, $RD_i = LD_{i-1} \oplus F(RD_{i-1}, K_{n-i+1})$
- $LD_i = RE_{n-i}$
- $RD_i = LE_{n-i}$

Generation of Round Keys from Master Key

- The round keys (sub-keys) K_i are derived from the master key K (The process is called Key-Expansion)
- Each Round uses a unique round-key.
- The Key-Expansion uses operations like Permutations, Substitutions, and other transformations.

Example 1

- Assume that the PT = 0x3C; $K_1 = 0xF$, $K_2 = 0xA$. $F(x,y) =$ Bitwise Logical AND of x and y. What are the outputs of the first 2 rounds of Feistel Cipher encryption?

Solution:-

- PT = 0x3C
- $LE_0 = (0011)_2$
- $RE_0 = (1100)_2$

Example 1 (Contd..)

Round 1:-

- $LE_1 = (1100)_2$
- $RE_1 = LE_0 \oplus F(RE_0, K_1)$
- $RE_1 = (0011)_2 \oplus F((1100)_2, (1111)_2)$
- $RE_1 = (0011)_2 \oplus (1100)_2$
- $RE_1 = (1111)_2$
- *Therefore, Round 1 Output = 0xCF*

Example 1 (Contd..)

Round 2:-

- $LE_2 = (1111)_2$
- $RE_2 = LE_1 \oplus F(RE_1, K_2)$
- $RE_2 = (1100)_2 \oplus F((1111)_2, (1010)_2)$
- $RE_2 = (1100)_2 \oplus (1010)_2$
- $RE_2 = (0110)_2$
- *Therefore, Round 2 Output = 0xF6.*

Example 2

- Assume that Feistel Cipher uses 16 rounds. The output of the 14th Round is 0x8D; $K_{15} = 0x7$, $K_{16} = 0xC$. $F(x,y) = \text{Logical OR of } x \text{ and } y$. Calculate CT.

Solution:-

- $LE_{14} = (1000)_2$
- $RE_{14} = (1101)_2$

Example 2 (Contd..)

Round 15:-

- $LE_{15} = RE_{14} = (1101)_2$
- $RE_{15} = LE_{14} \oplus F(RE_{14}, K_{15})$
- $RE_{15} = (1000)_2 \oplus F((1101)_2, (0111)_2)$
- $RE_{15} = (1000)_2 \oplus (1111)_2$
- $RE_{15} = (0111)_2$

Example 2 (Contd..)

Round 16:-

- $LE_{16} = RE_{15} = (0111)_2$
 - $RE_{16} = LE_{15} \oplus F(RE_{15}, K_{16})$
 - $RE_{16} = (1101)_2 \oplus F((0111)_2, (1100)_2)$
 - $RE_{16} = (1101)_2 \oplus (1111)_2$
 - $RE_{16} = (0010)_2$
 - Output of Round 16 = 0x72
-
- *Therefore, CT = 0x27*

Example 3

- Assume that Feistel Cipher uses 16 rounds. The CT is 0xAB, $K_{16} = 0x7$. The Round Function $F(x,y) = \text{bitwise XOR (1-bit right rotation of } x, \text{ 1-bit right rotation of } y)$. What's the output of the first round during decryption?

Solution:-

- $LD_0 = (1010)_2$
- $RD_0 = (1011)_2$

Example 3 (Contd..)

- $LD_1 = RD_0 = (1011)_2$
 - $RD_1 = LD_0 \oplus F(RD_0, K_{16})$
 - $RD_1 = (1010)_2 \oplus F((1011)_2, (0111)_2)$
 - $RD_1 = (1010)_2 \oplus ((1101)_2 \oplus (1011)_2)$
 - $RD_1 = (1010)_2 \oplus (0110)_2$
 - $RD_1 = (1100)_2$
-
- *Therefore, Output of First Round of decryption is 0xBC.*

Example 4

- Assume that Feistel Cipher uses 16 rounds. The output of 15th Round of decryption is 0xABCD, $K_1 = 0xE9$. The Round Function $F(x,y) =$ bitwise XOR (bitwise NOT of x, bitwise NOT of y). What's the deciphered text?

Solution:-

- $LD_{15} = 0xAB = (10101011)_2$
- $RD_{15} = 0xCD = (11001101)_2$
- $K_1 = (11101001)_2$

Example 4 (Contd..)

- $LD_{16} = RD_{15} = (11001101)_2$
 - $RD_{16} = LD_{15} \oplus F(RD_{15}, K_1)$
 - $RD_{16} = (10101011)_2 \oplus F[(11001101)_2, (11101001)_2]$
 - $RD_{16} = (10101011)_2 \oplus [(00110010)_2 \oplus (00010110)_2]$
 - $RD_{16} = (10101011)_2 \oplus (00100100)_2$
 - $RD_{16} = (10001111)_2 = 0x8F$
-
- *Therefore, the Deciphered text is 0x8FCD*

S-BOXES AND P-BOXES



S-Boxes

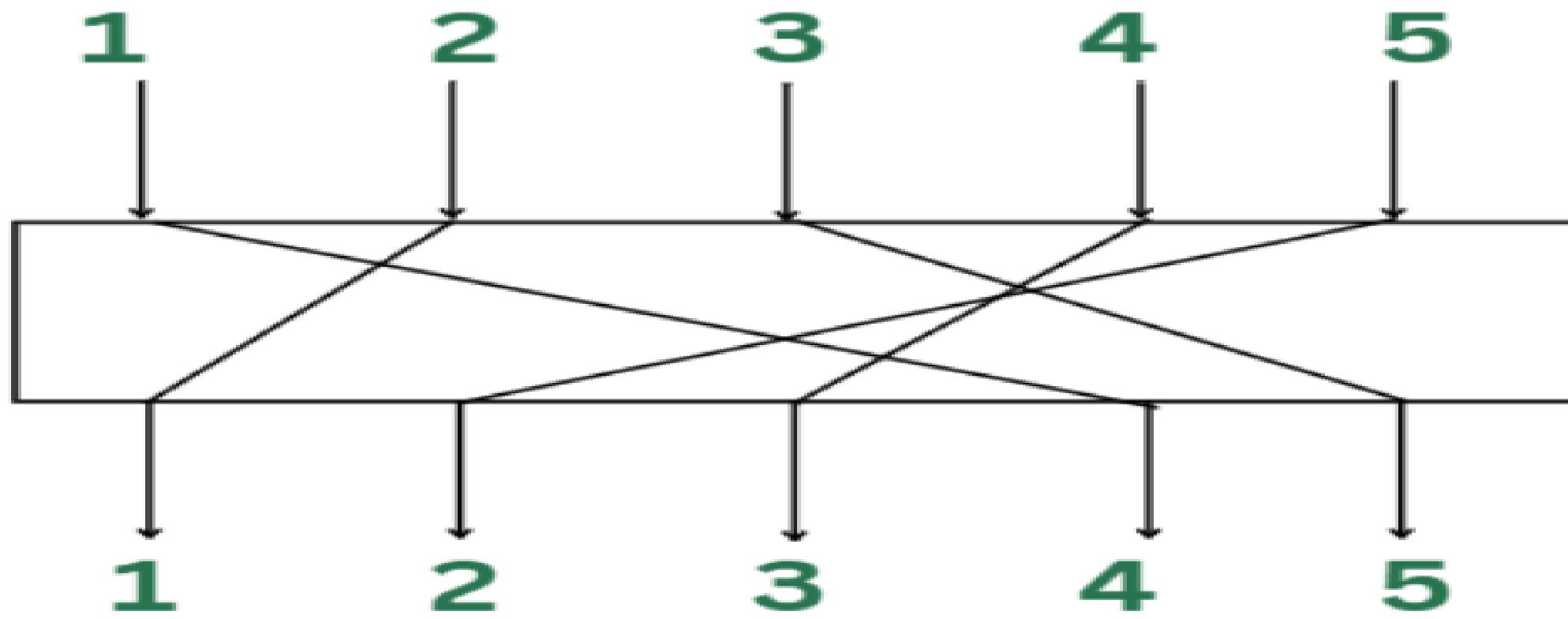
- Uses Non-Linear Transformation to generate Outputs from Inputs.
 - Mapping between inputs and corresponding outputs are defined by a table or a matrix.
 - It should be such that its not easily invertible by an attacker.
 - Two main categories of S-Boxes:- Static S-Box and Dynamic S-Box
-



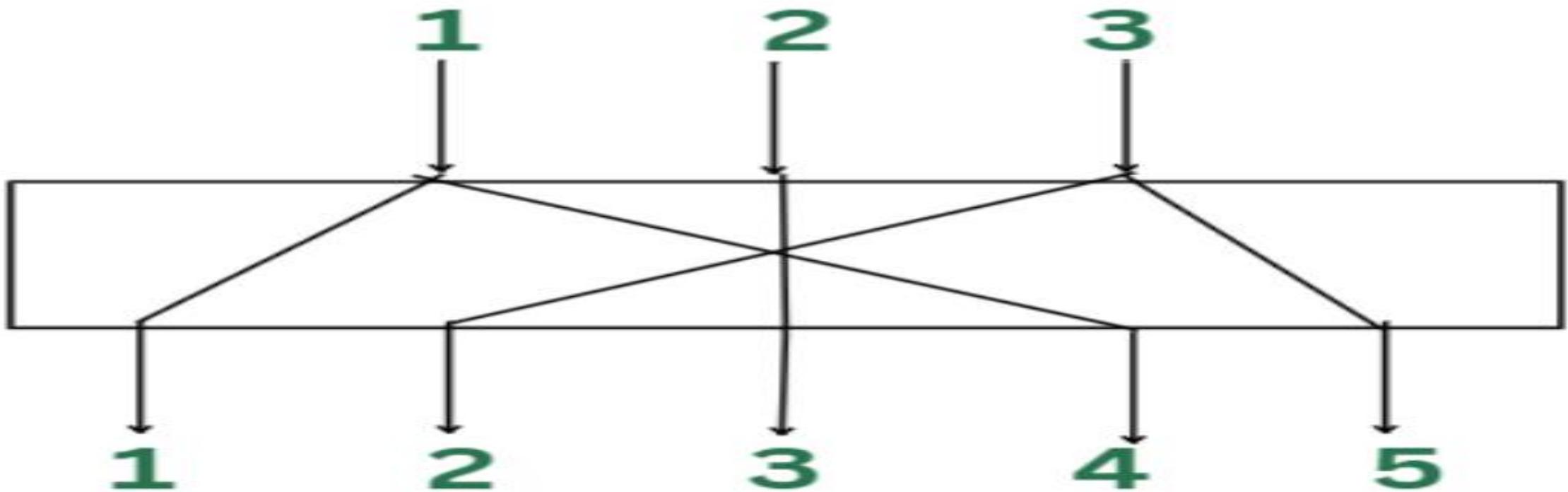
P-Boxes

- The primary goal is to increase diffusion for a cipher, by permuting the input bits.
 - Permutation of the bits makes the cryptanalysis more challenging.
 - Types of P-Boxes: Straight P-Box, Compression P-Box, and Expansion P-Box.
-

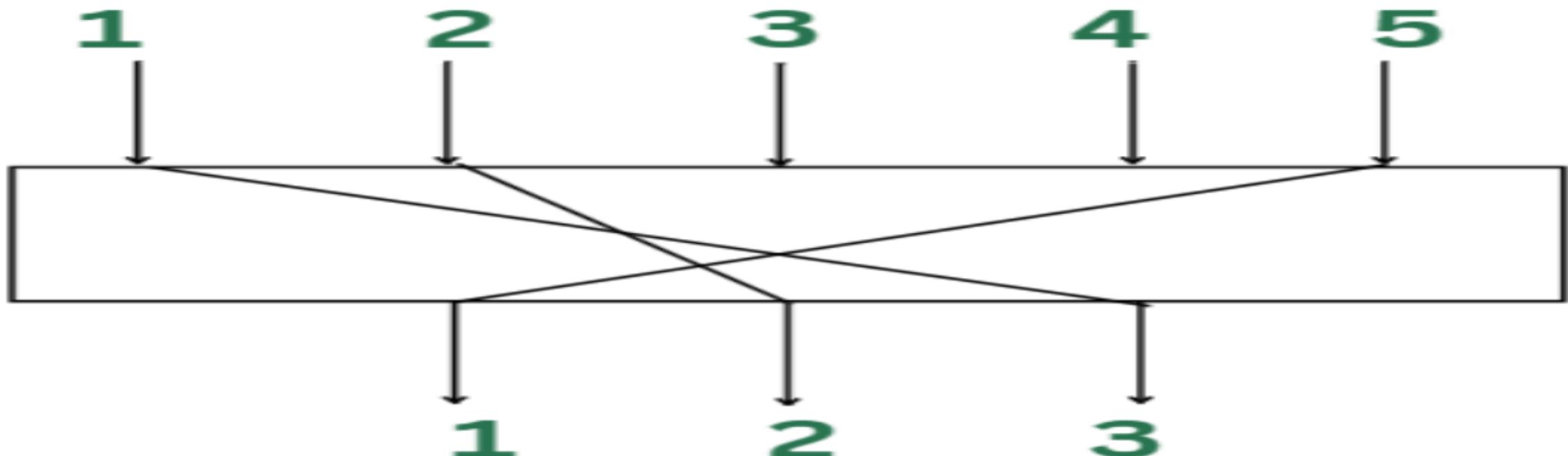
Straight P-Box



Expansion P-Box



Compression P-Box

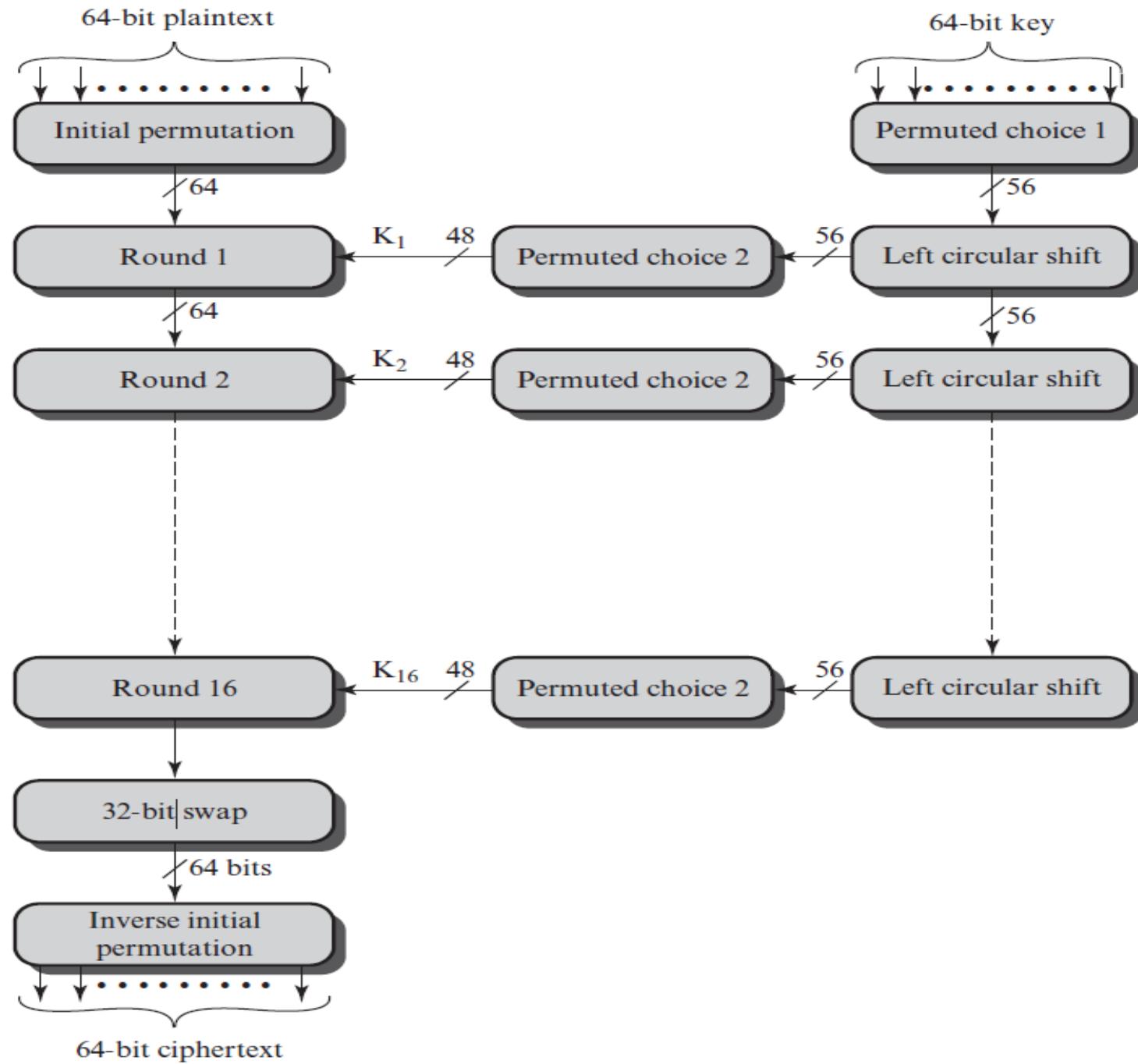


Data Encryption Standard (DES)

DES

- Developed by IBM.
- Adopted as a federal standard by NIST in 1977.
- Input = 64-bit block
- Output = 64-bit block
- Original Key Length = 64 bits
- Effective Key Length = 56 bits
- Round Key = 48 bits
- Consists of 16 rounds.
- Each Round consists of different operations like Substitution, Permutation, Key-Mixing, and Expansion.

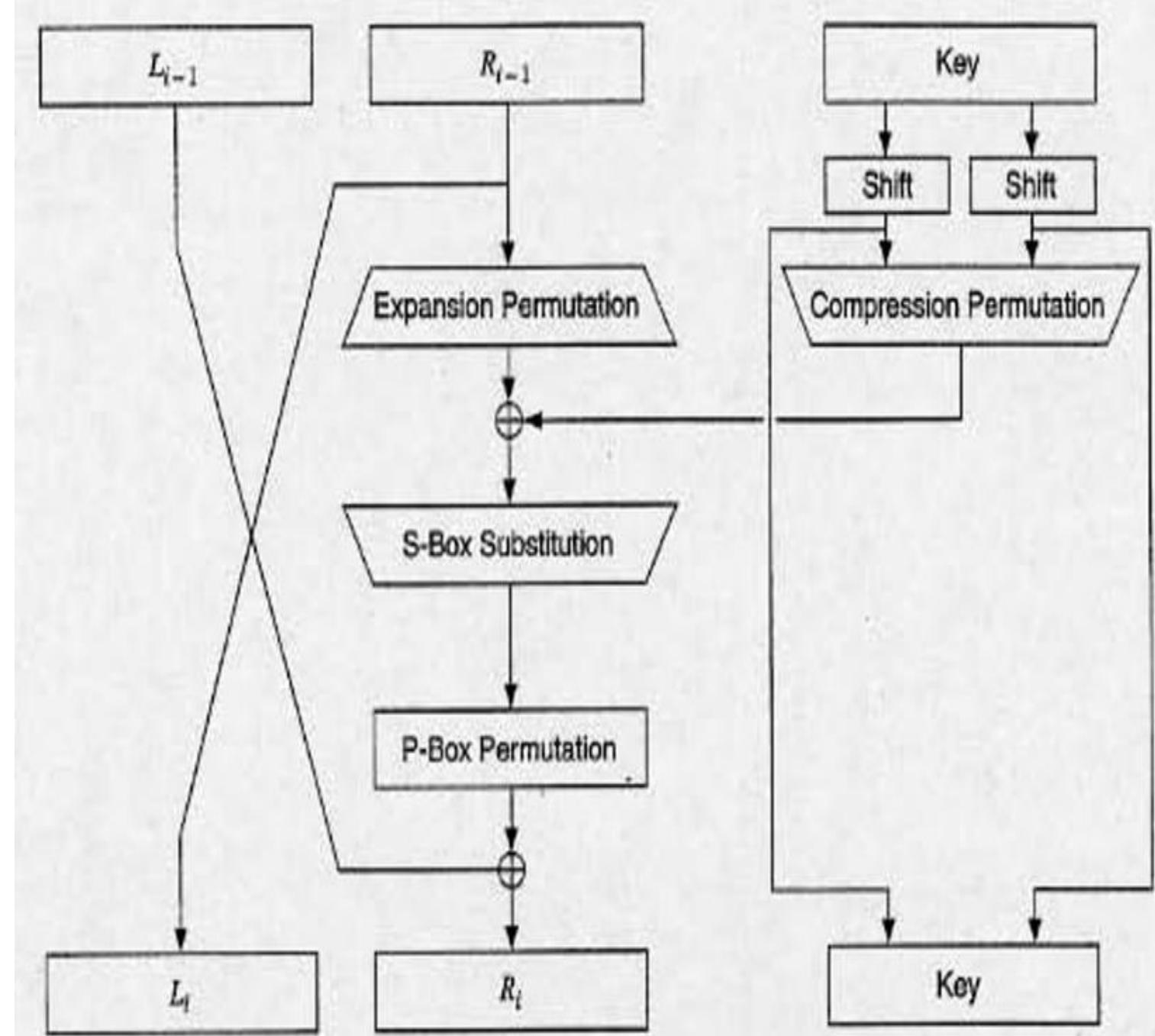
DES Encryption



DES Decryption



One Round of DES





Example 1

- PT 1 = 0x46868bd449786458
- Key 1 = 0x144573e006467894
- CT 1 = 0xae8180eb706729d3

- Key 2 = 0x144573e016467894
- CT 2 = 0xa14a01e6c590db61



Example 2

- PT 1 = 0xfedcba9876543210
 - Key 1 = 0x0123456789abcdef
 - CT 1 = 0x12c626af058b433b

 - PT 2 = 0xfedcba9876543211
 - CT 2 = 0x7b129948ca8d29d6
-

Strength of DES

- Number of possible keys = $7.2057 * 10^{16}$.
- Maximum time required for a PC to execute a successful DES decryption at 10^9 decryptions/second = $(7.2057 * 10^{16})/(10^9/\text{second}) = 7.2057 * 10^7$ seconds ≈ 2 years and 3 months.
- Cryptanalysis is possible by exploiting the characteristics of DES.
- DES is moderately resistant to a successful timing attack.