Applied Cryptography

By:
Dr. Archana Gupta

Security Goals

Confidentiality

- It is the most common aspect of Information Security.
- To protect our confidential information
- In military , concealment of its information is major concern
- In banking, customer accounts need to be secret

Integrity

- Information needs to change constantly.
- When a customer deposit or withdraw money, balance needs to be updated.
- Data integrity

  Assures that information and programs are changed only in a specified and authorized manner
  - System integrity

  Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system

Availability

- The information created and stored by an organization needs to be available to authorized entities.
- Information is useless if it is not available.
- Customer not able to do transactions or check balance

Three aspects of information security

- Security attack – Any action that compromises the security of information owned by an organization.

- Security mechanism – A mechanism that is designed to detect, prevent or recover from a security attack. 1.Encipherment 2 Digital Signature 3 Access Control

- Security service – A service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks and they make use of one or more security mechanisms to provide the service.

Threat

A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.

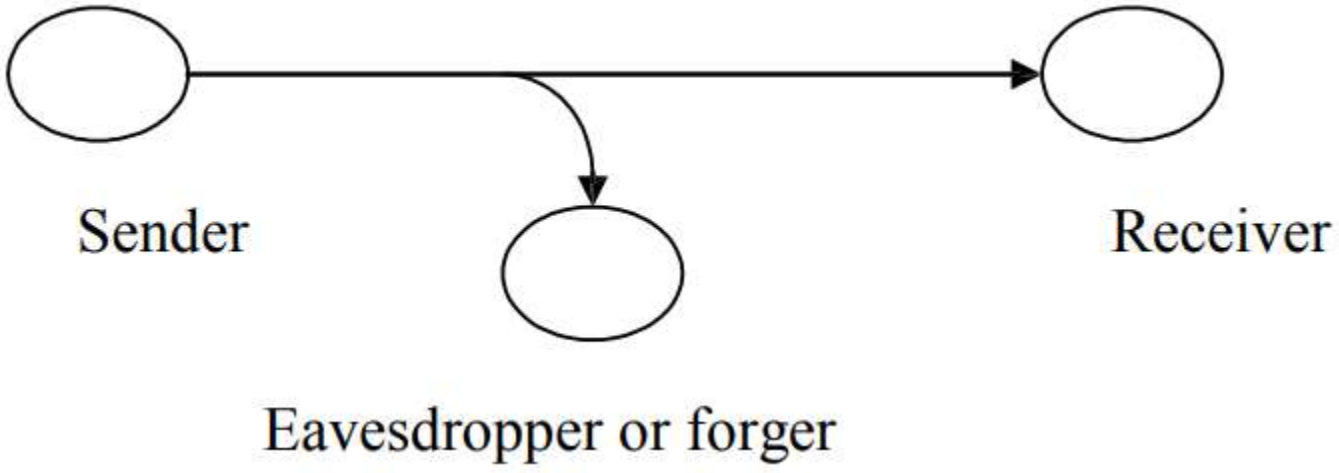
Attack

An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

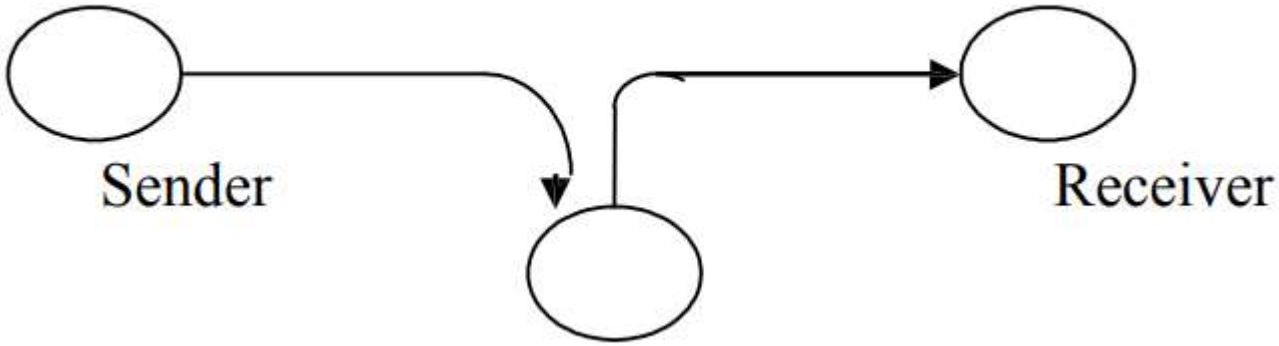
SECURITY ATTACKS

- There are four general categories of attack:
- Interruption : An asset of the system is destroyed or becomes unavailable or unusable. This is an attack on availability e.g., destruction of piece of hardware, cutting of a communication line or Disabling of file management system.

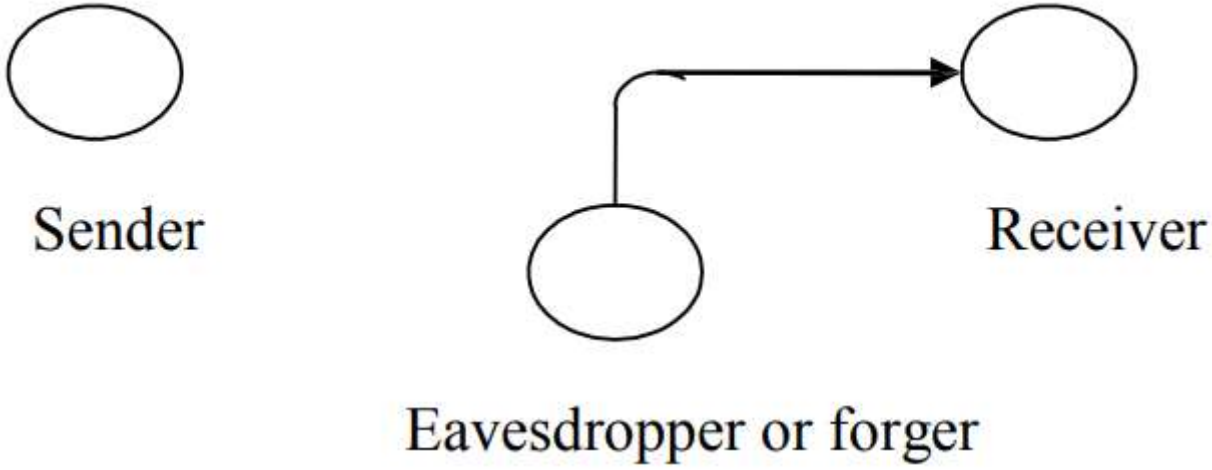
- Interception :
- An unauthorized party gains access to an asset. This is an attack on confidentiality. Unauthorized party could be a person, a program or a computer.e.g., wire tapping to capture data in the network, illicit copying of files



- Modification :
- An unauthorized party not only gains access to but tampers with an asset. This is an attack on integrity. e.g., changing values in data file, altering a program, modifying the contents of messages being transmitted in a network.



- Fabrication :
- An unauthorized party inserts counterfeit objects into the system. This is an attack on authenticity. e.g., insertion of spurious message in a network or addition of records to a file.



Cryptographic Attacks

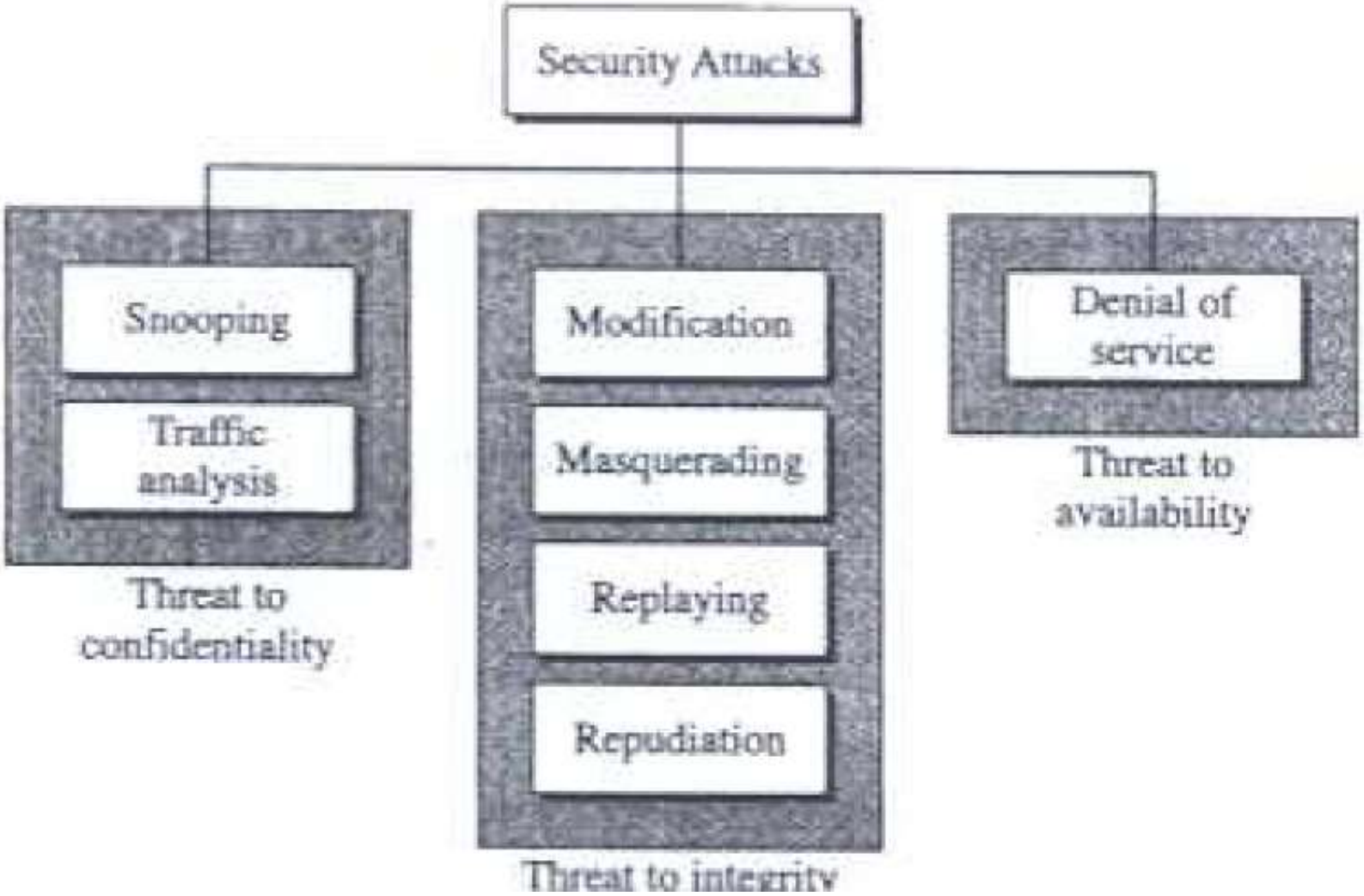
- Cryptanalytic Attacks – Algorithms based
- Non-Cryptanalytic Attacks – don’t exploit the mathematical weakness

Passive Versus Active Attacks

- Passive- Attacker goal is to obtain information
- Active – change the data or harm the system

Attacks	*Passive/Active*	*Threatening*
Snooping Traffic analysis	Passive	Confidentiality
Modification Masquerading Replaying Repudiation	Active	Integrity
Denial of service	Active	Availability

Taxonomy of attacks wrt security goals



Attacks Threatening Confidentiality

- Snooping – unauthorized access or interception of data. Can use encipherment techniques to make data nonintelligible.
- Traffic Analysis- obtain some other type of information by monitoring traffic. Ex- Nature of transaction, mail ids of receiver or sender

Attacks Threatening Integrity

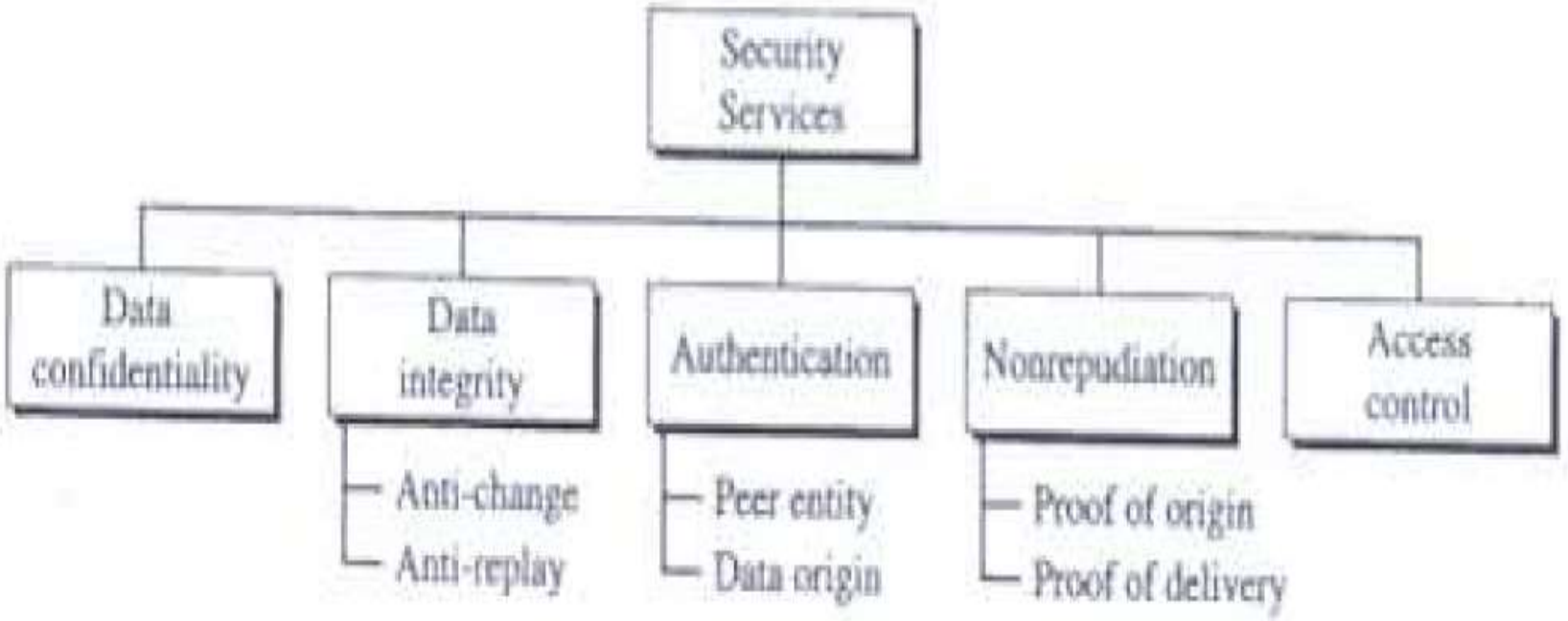
- Modification- attacker modifying the request of customer to bank
- Masquerading- attacker impersonate somebody. Ex-steal card and use card and pin
- Replaying- somebody sent message to bank to pay to a person X and X is sending that message agin to the bank for payment again.
- Repudiation- denial by either sender or receiver. Ex- A customer send the message to bank to make payment to third party and lateron denying on it.

Attacks threatening availability

- Denial of Service- . It may slow down or totally interrupt the service of a system. send so many bogus requests to a server that the server crashes because of the heavy load. The attacker might intercept and delete a server's response to a client, making the client to believe that the server is not responding. The attacker may also intercept requests from the clients, causing the clients to send requests many times and overload the system.

Services and Mechanism

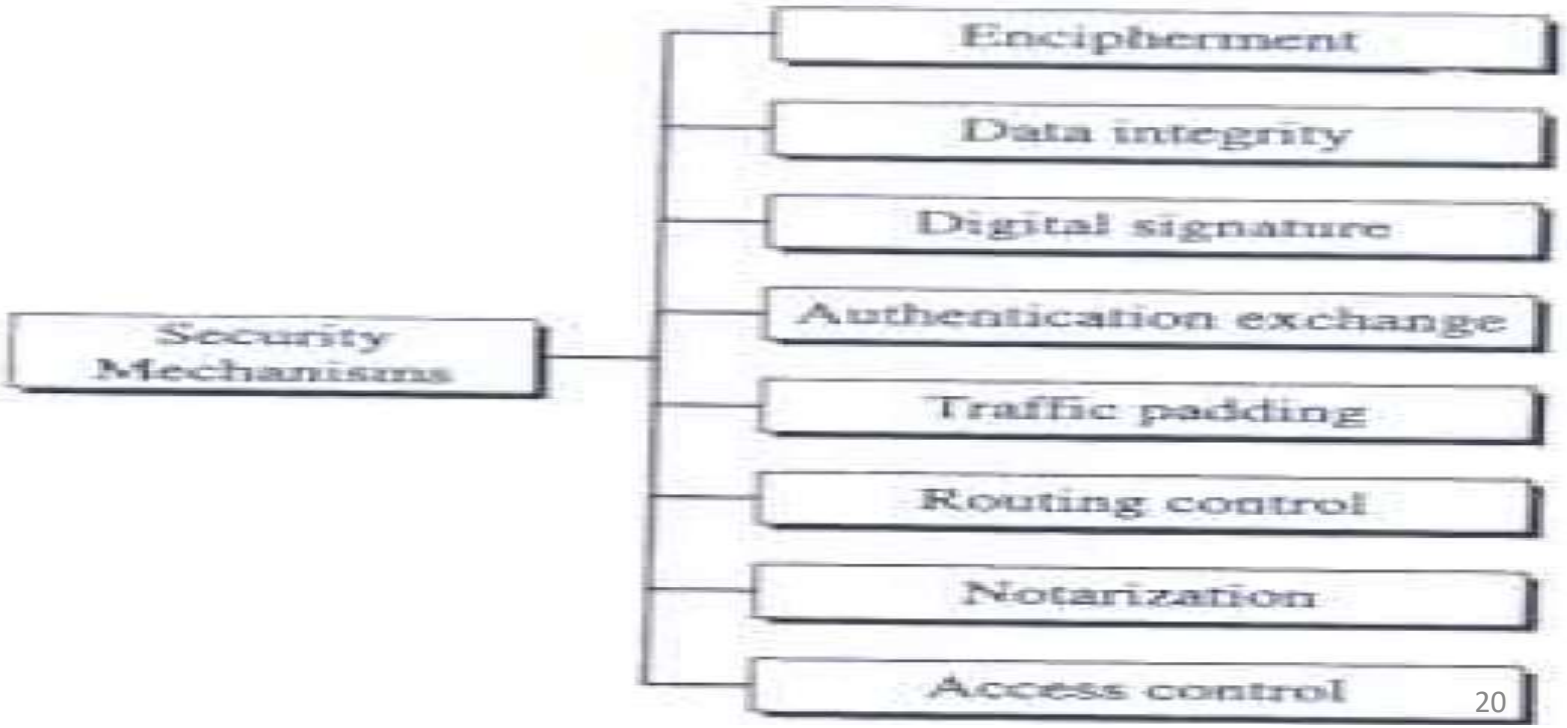
- Mechanism or its combination is used to Security Services



- Data confidentiality is designed to protect data from disclosure attack. it is designed to prevent snooping and traffic analysis attack.
- Data integrity is designed to protect data from modification, insertion, deletion, and replaying by an adversary. It may protect the whole message or part of the message.
- Authentication This service provides the authentication of the party at the other end of the line. In Connection-oriented communication, it provides authentication of the sender or receiver
- Nonrepudiation service protects against repudiation by either the sender or the receives of the data. In nonrepudiation with proof of the origin, the receiver of the data can lateron prove the identity of the sender if denied. In nonrepudiation with proof of delivery, the sender of data can later prove that data were delivered to the intended recipient.
- Access Control Access control provides protection against unauthorized access to data. The terms access in this definition is very broad and can involve reading, writing, modifying, executing programs, and so on.

Security Mechanism

- The International Telecommunication Union-Telecommunication Standardization Sector ITU-T (X.800) also recommends some security mechanisms to provide the security services



Number Theory

- The goal of every cryptographic scheme is to be "crack proof"
- Cryptography is also a means to ensure the integrity and preservation of data from tampering.
- Modern cryptographic systems relies highly on functions associated with advanced mathematics, including number theory
- Number Theory explores the properties of numbers and the relationships between numbers.

Why?

- prime numbers and functions related to prime numbers

Objectives

- To study integer arithmetic, concentrating on divisibility and finding the greatest common divisor using the Euclidean algorithm
- To understand how the extended Euclidean algorithm can be used to solve linear congruent equations, and to find the multiplicative inverses
- To emphasize the importance of modular arithmetic and the modulo operator
- To emphasize and review matrices and operations on residue matrices that are extensively used in cryptography
- To solve a set of congruent equations using residue matrices

Cryptography is based on some specific areas of mathematics, including number theory, linear algebra, and algebraic structures.

INTEGER ARITHMETIC

- Concept of set and a few operations.
- Set of Integers
- Binary Operations
- Integer Division
- Divisibility
  - Euclidean Algorithm
  - The Extended Euclidean Algorithm

Set of Integers

- Set of Integers

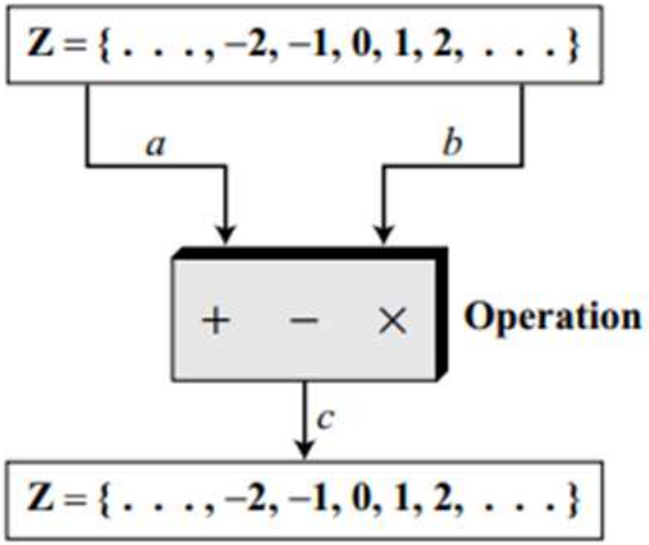
The set of integers contains all integral numbers (with no fraction) from negative infinity to positive infinity

$Z = \{ \ldots, -2, -1, 0, 1, 2, \ldots \}$

Binary Operations

- Three binary operations applied to the set of integers : addition, subtraction, and multiplication, division
- A binary operation takes two inputs and creates one output.
- Each operations takes two inputs (a and b) and creates one output (c)
- The two inputs come from the set of integers; the output goes into the set of integers

Figure 2.2 *Three binary operations for the set of integers*



Example 2.1

The following shows the results of the three binary operations on two integers. Because each input can be either positive or negative, we can have four cases for each operation.

Add:	$5 + 9 = 14$	$(-5) + 9 = 4$	$5 + (-9) = -4$	$(-5) + (-9) = -14$
Subtract:	$5 - 9 = -4$	$(-5) - 9 = -14$	$5 - (-9) = 14$	$(-5) - (-9) = +4$
Multiply:	$5 \times 9 = 45$	$(-5) \times 9 = -45$	$5 \times (-9) = -45$	$(-5) \times (-9) = 45$

Integer Division

- The division produces two outputs instead of one: Quotient and Remainder
- The operation a ÷ n gives q and r.
- The relationship between these four integers:

$a = q \times n + r$

- a => dividend;
- Q => quotient;
- N => divisor
- R => remainder.
- Division is not taken as an operation, because the result of dividing a by n is two integers, q and r.
- It is taken as division relation

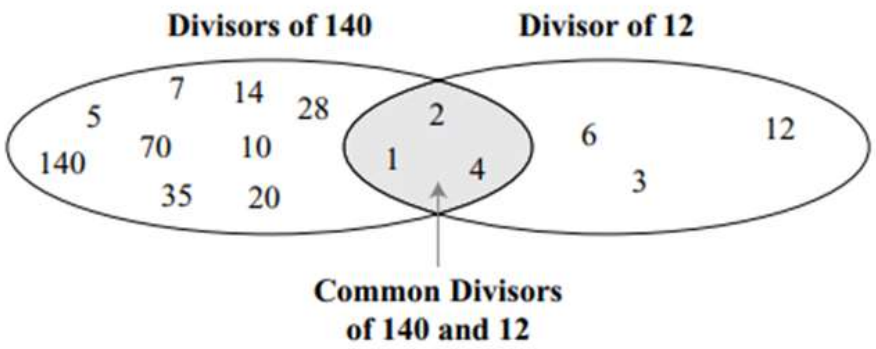
Divisibility

- Depends on if r=0 in the division relation
- a | n if a is divisible by n
- a ∤ n otherwise

Property 1: if $a|1$, then $a = \pm 1$.
Property 2: if $a|b$ and $b|a$, then $a = \pm b$.
Property 3: if $a|b$ and $b|c$, then $a|c$.
Property 4: if $a|b$ and $a|c$, then $a|(m \times b + n \times c)$, where m and n are arbitrary integers.

Greatest Common Divisor

- Two positive integers may have many common divisors, but only one greatest common divisor.
- E.g. the common divisors of 12 and 140 are 1, 2, and 4. However, the greatest common divisor is 4.
- The greatest common divisor of two positive integers is the largest integer that can divide both integers.
-



Euclidean Algorithm

- Finding gcd of two positive integers by listing all common divisors is not practical when the two integers are large.
- Euclid(BC 300) developed an algorithm to find the GCD of two positive integers.

Fact 1: gcd $(a, 0) = a$

Fact 2: gcd (a, b) = gcd (b, r), where r is the remainder of dividing a by b

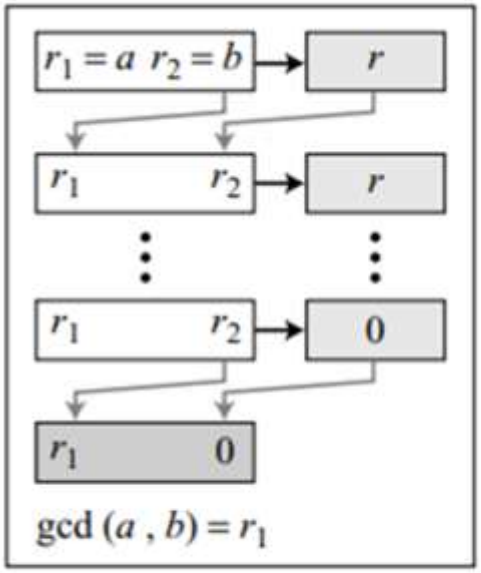
---

Euclidean Algorithm

- Fact 1: if the second integer is 0, the greatest common divisor is the first one.
- Fact 2: allows us to change the value of a, b until b becomes 0
- E.g. calculate gcd (36, 10). (use the second fact several times)

gcd (36, 10) = gcd (10, 6) = gcd (6, 4) = gcd (4, 2) = gcd (2, 0) = 2

Euclidean Algorithm



a. Process

```
r1 ← a; r2 ← b;  (Initialization)
while (r2 > 0)
 {
  q ← r1 / r2;
  r ← r1 - q × r2;
  r1 ← r2; r2 ← r;
 }

  gcd (a, b) ← r1
```

b. Algorithm

- When gcd (a, b) = 1, a and b are termed as relatively prime.

Euclidean Algorithm

Example 2.7

Find the greatest common divisor of 2740 and 1760.

Solution

We apply the above procedure using a table. We initialize r_1 to 2740 and r_2 to 1760. We have also shown the value of q in each step. We have gcd (2740, 1760) = 20.

q	r_1	r_2	r
1	2740	1760	980
1	1760	980	780
1	980	780	200
3	780	200	180
1	200	180	20
9	180	20	0
	20	0	

The Euclidean Algorithm

Example 2.8

Find the greatest common divisor of 25 and 60.

Solution

We chose this particular example to show that it does not matter if the first number is smaller than the second number. We immediately get our correct ordering. We have gcd (25, 65) = 5.

q	r_1	r_2	r
0	25	60	25
2	60	25	10
2	25	10	5
2	10	5	0
	5	0	

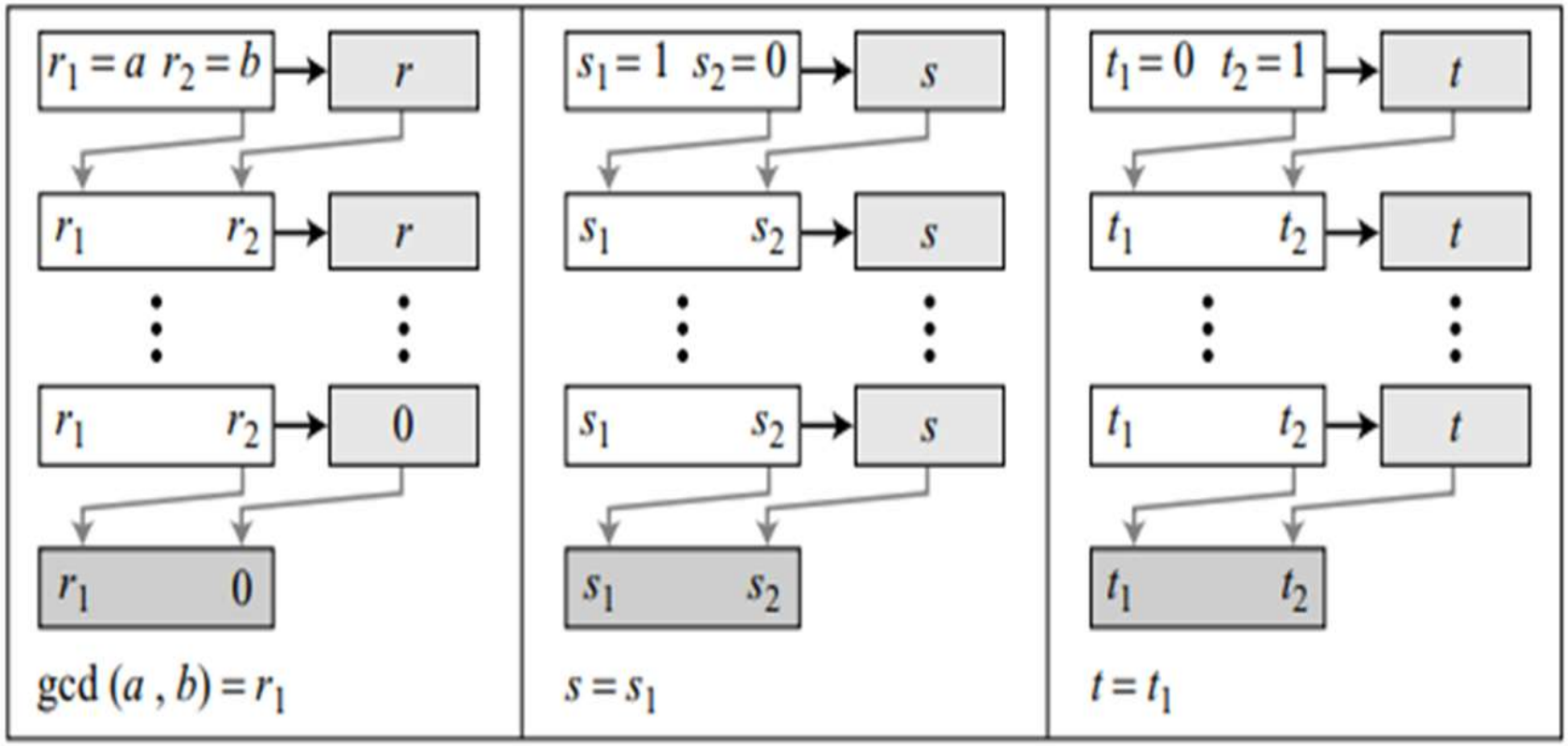
The Extended Euclidean Algorithm

- Given two integers a and b, the extended Euclidean algorithm helps to find other two integers, s and t, such that

$$\mathbf{s \times a + t \times b = gcd\ (a, b)}$$

- The extended Euclidean algorithm can calculate the gcd (a, b) and at the same time calculate the value of s and t.
- **Used extensively in computing multiplicative inverses in simple algebraic field extensions**.

Extended Euclidean Algorithm to find GCD



Extended Euclidean Algorithm

```
r1 ← a; r2 ← b;
s1 ← 1; s2 ← 0;          (Initialization)
t1 ← 0; t2 ← 1;
while (r2 > 0)
{
  q ← r1 / r2;
  r ← r1 − q × r2;
  r1 ← r2;  r2 ← r;      (Updating r's)
  s ← s1 − q × s2;
  s1 ← s2;  s2 ← s;      (Updating s's)
  t ← t1 − q × t2;
  t1 ← t2;  t2 ← t;      (Updating t's)
}
 gcd (a , b) ← r1;   s ← s1;   t ← t1
```

Extended Euclidean Algorithm Examples

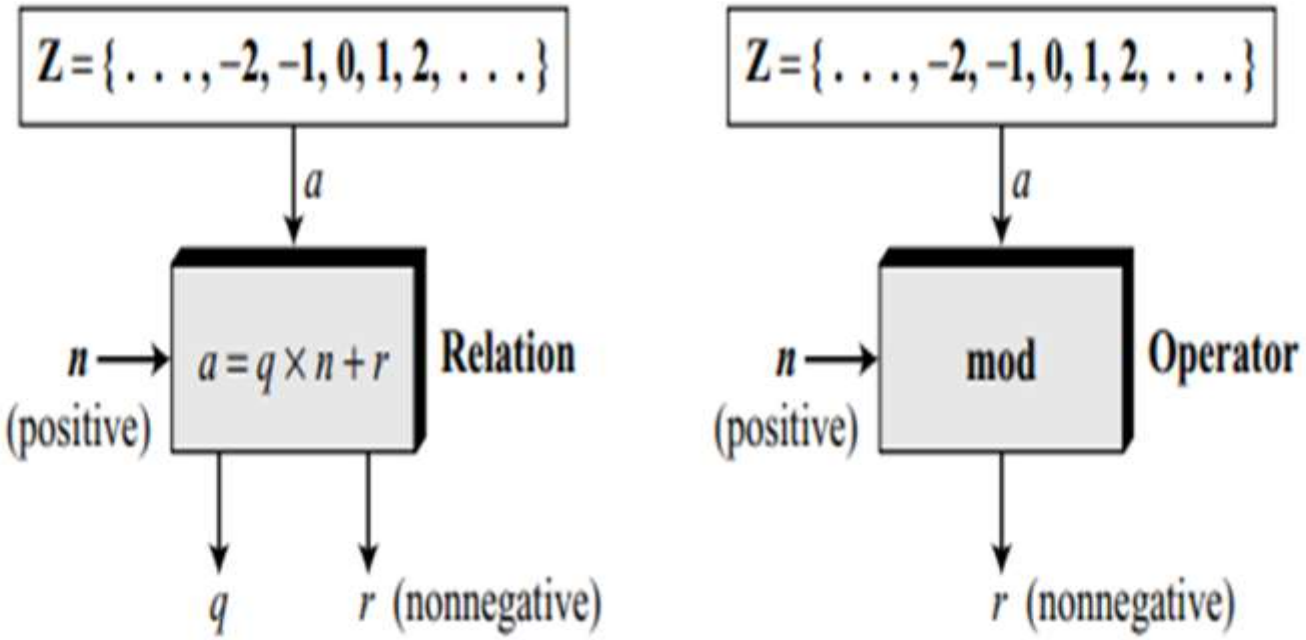
••Given a = 161 and b = 28, find gcd (a, b). •GCD(161,28)=7

Q=r1/r2	R1	R2	R	s1	s2	s= s1 − q × s2	T1	T2	T=t1 − q × t2
5	161	28	21	1	0	1	0	1	-5
1	28	21	7	0	1	-1	1	-5	6
3	21	7	0	1	-1	4	-5	6	-23
	7	0		-1	4		6	-23	6

MODULAR ARITHMETIC

- The modular arithmetic is interested in only one of the outputs, the remainder r.
- The quotient q is not significant
- Mod=modulo operator
- a mod n ⇒ The second input (n) is called the modulus.
- r= a mod n ⇒ The output r is called the residue.

Division relation and modulo operator



Set of Residues: Zn

- The result of the modulo operation with modulus n is always an integer between 0 and n − 1.
- i.e. result of a mod n is always a nonnegative integer < n.
- i.e. modulo operation creates a set, referred to as the set of least residues modulo n, or Z_n.

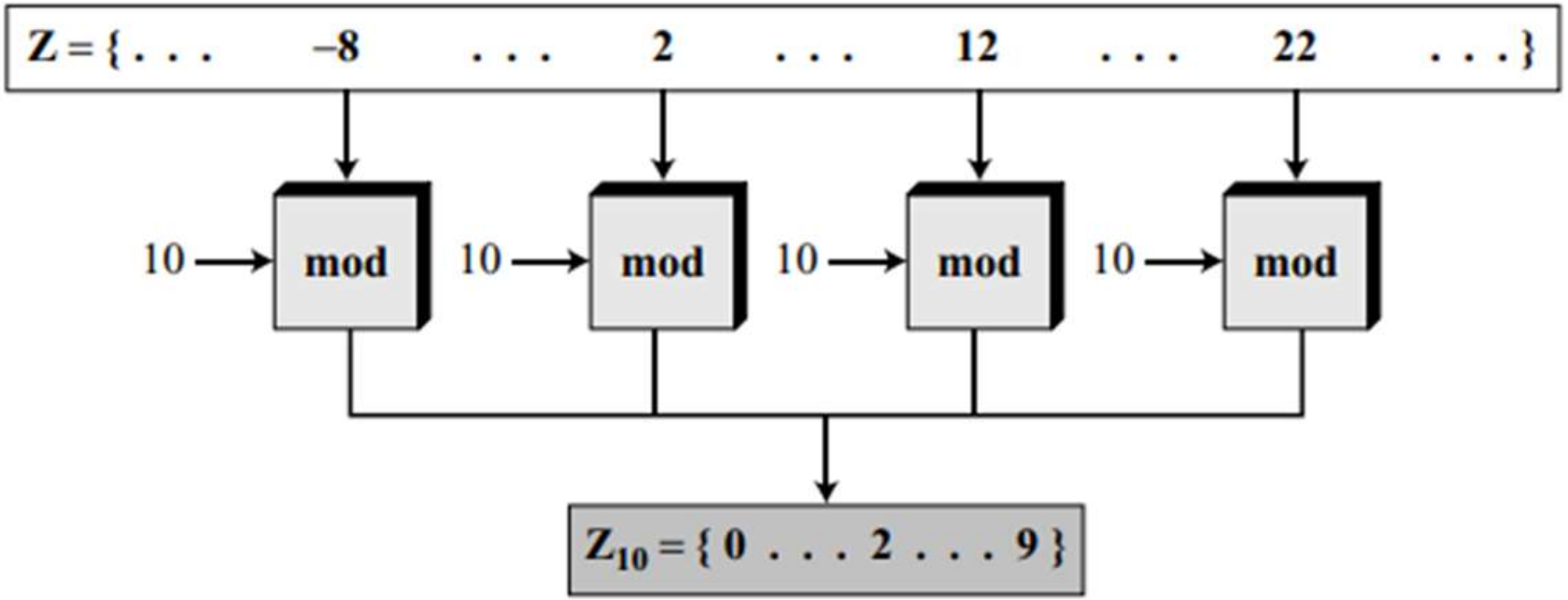
$Z_n = \{ 0, 1, 2, 3, \ldots, (n - 1) \}$

- $Z_2 = \{ 0, 1 \}$
- $Z_6 = \{ 0, 1, 2, 3, 4, 5 \}$
- $Z_{11} = \{ 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 \}$

Congruence

- Cryptography uses the concept of congruence instead of equality.
- Mapping from Z to Z_n is not one-to-one.
- Infinite members of Z can map to one member of Z_n.
- E.g. , 2 mod 10 = 2, 12 mod 10 = 2, 22 mod 2 = 2, and so on.
- Hence in modular arithmetic, integers like 2, 12, and 22 are called congruent mod 10.
- Denoted with **congruence operator (≡).**
- $2 \equiv 12 \pmod{10}$, $13 \equiv 23 \pmod{10}$, $34 \equiv 24 \pmod{10}$,
- $-8 \equiv 12 \pmod{10}$, $3 \equiv 8 \pmod{5}$, $8 \equiv 13 \pmod{5}$,

  $23 \equiv 33 \pmod{5}$, $-8 \equiv 2 \pmod{5}$



$$-8 \equiv 2 \equiv 12 \equiv 22 \pmod{10}$$

Congruence Relationship

A residue class

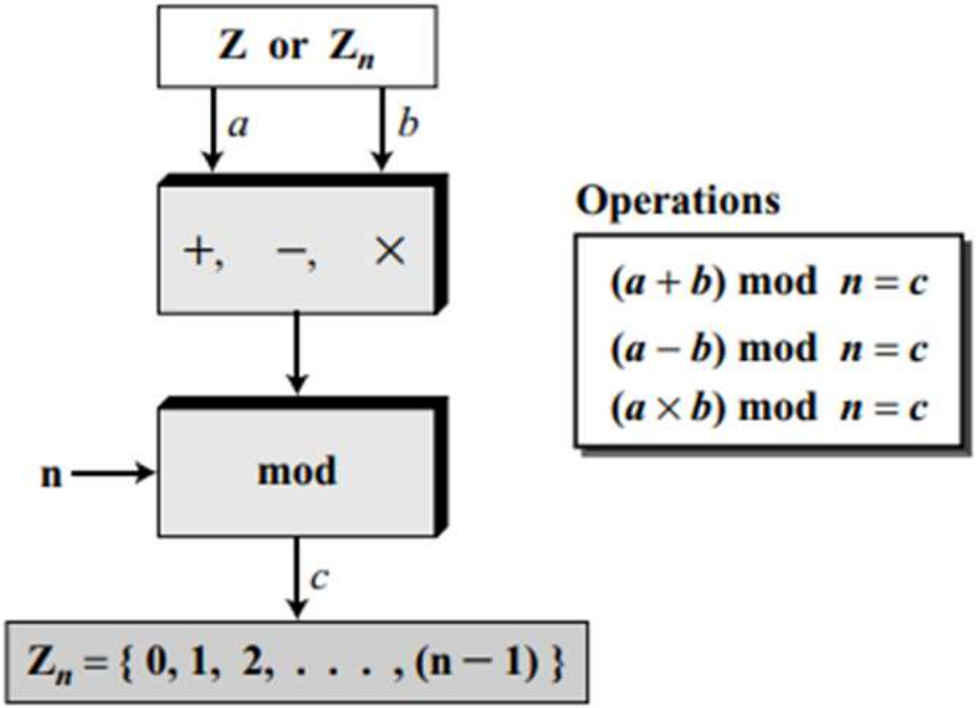
- A residue class [a] or [a]n is the set of integers congruent modulo n.
- i.e. the set of all integers x such that

$$x = a \pmod{n}.$$

- E.g. n = 5, gives five sets [0], [1], [2], [3], and [4] as :
- [0] = {…, −15, −10, −5, 0, 5, 10, 15, …}
- [1] = {…, −14, −9, −4, 1, 6, 11, 16, …}
- [2] = {…, −13, −8, −3, 2, 7, 12, 17, …}
- [3] = {…, −12, −7, −5, 3, 8, 13, 18, …}
- [4] = {…, −11, −6, −1, 4, 9, 14, 19, …}
- The set of all of these least residues: $Z_5 = \{0, 1, 2, 3, 4\}$.
- i.e, the set Z_n is the set of all least residue modulo n.

Operations in Z_n

- Addition, subtraction, and multiplication can also be defined for the set Zn.



Example operations over Zn

1.Add 7 to 14 in Z15.

Solution: (14 + 7) mod 15 → (21) mod 15 = 6

2.Subtract 11 from 7 in Z13.

(7 − 11) mod 13 → (−4) mod 13 = 9 (Additive inverse)

3. Multiply 11 by 7 in Z20

(7 × 11) mod 20 → (77) mod 20 = 17

Example operations over Zn

Example 2.17

Perform the following operations (the inputs come from either **Z** or $\mathbf{Z}_n$):

a. Add 17 to 27 in $\mathbf{Z}_{14}$.

b. Subtract 43 from 12 in $\mathbf{Z}_{13}$.

c. Multiply 123 by −10 in $\mathbf{Z}_{19}$.

Solution

The following shows the two steps involved in each case:

$$(17 + 27) \bmod 14 \rightarrow (44) \bmod 14 = 2$$
$$(12 - 43) \bmod 13 \rightarrow (-31) \bmod 13 = 8$$
$$(123 \times (-10)) \bmod 19 \rightarrow (-1230) \bmod 19 = 5$$

Inverses

- modular arithmetic often needs to find the inverse of a number relative to an operation.
- Types:
  - additive inverse (relative to an addition operation) or
  - a multiplicative inverse (relative to a multiplication

Additive Inverse In Z_n

- In Z_n, two numbers a and b are additive inverses of each other if

$$a + b \equiv 0 \pmod{n}$$

- The additive inverse of a can be calculated as

$$b = n - a.$$

- E.g. the additive inverse of 4 in Z_{10} is $10 - 4 = 6$.

In modular arithmetic, each integer has an additive inverse.
The sum of an integer and its additive inverse is congruent to 0 modulo *n*.

- Find all additive inverse pairs in Z_{10}

Solution: The six pairs of additive inverses are :

(0, 0), (1, 9), (2, 8), (3, 7), (4, 6), and (5, 5).

- 0 is the additive inverse of itself; so is 5.
- Note : the additive inverses are reciprocal;

– E.g. if 4 is the additive inverse of 6, then 6 is also the additive inverse of 4.

Additive inverse of –ve number

- Formula : $-n \bmod k \equiv k - (n \bmod k)$
- e.g. $-3 \bmod 12 = 12 - (3 \bmod 12) = 12 - 3 = 9$
- $-34 \bmod 23 = 23 - (34 \bmod 23) = 23 - 11 = 12$
-

Hint: if $n < k$, compute $k-n$

- else take multiple of k which is just greater than n, subtract n from that multiple
- e.g. $23 * 2 = 46 > n=34 \Rightarrow 46-34 = 12$
-

Multiplicative Inverse

- In Zn, two numbers a and b are the multiplicative inverse of each other if

$$a \times b \equiv 1 \pmod{n}$$

- E.g. , if the modulus is 10, then the multiplicative inverse of 3 is 7.
  - i.e. (3 × 7) mod 10 = 1.
- a has a multiplicative inverse in Zn

iff gcd (n, a) = 1. i.e, a and n are relatively prime.

Multiplicative Inverse

In modular arithmetic, an integer may or may not have a multiplicative inverse. When it does, the product of the integer and its multiplicative inverse is congruent to 1 modulo *n*.

Multiplicative inverse

- Given two integers a and m, find the modular multiplicative inverse of a under modulo m.
- The modular multiplicative inverse is an integer X such that:

$a*x \equiv 1 \pmod{m}$

If a=3, m=11 then x= 4 , 3 and 4 are called multiplicative inverses of each other modulo 11

Modular multiplicative inverse when M and A are coprime i.e. gcd(a, m)=1

Example

- Find 4^{-1} mod 23
- So 4* x = 1 (mod 23)

4* 1 = 4 mod 23 = 4

4*2 = 8 mod 23 = 8

4*3 =12 mod 23 =12

4*4 =16 mod 23 = 16

4*5 = 20 mod 23 =20

4*6 = 24 mod 23 =1

So 4 & 6 are modulo inverses of each other modulo 23

Examples

- Find the multiplicative inverse of 8 in Z10.

Solution:

There is no multiplicative inverse because

gcd (10, 8) = 2 ≠ 1.

i.e. there exist no number between 0 and 9 such that when multiplied by 8, the result is congruent to 1.

Examples

- Find all multiplicative inverses in Z10.

Solution : (1, 1), (3, 7) and (9, 9).

The numbers 0, 2, 4, 5, 6, and 8 do not have a multiplicative inverse.

Examples

- Find all multiplicative inverse pairs in Z_{11}.

Solution: (1, 1), (2, 6), (3, 4), (5, 9), (7, 8), (9, 9), and (10, 10).

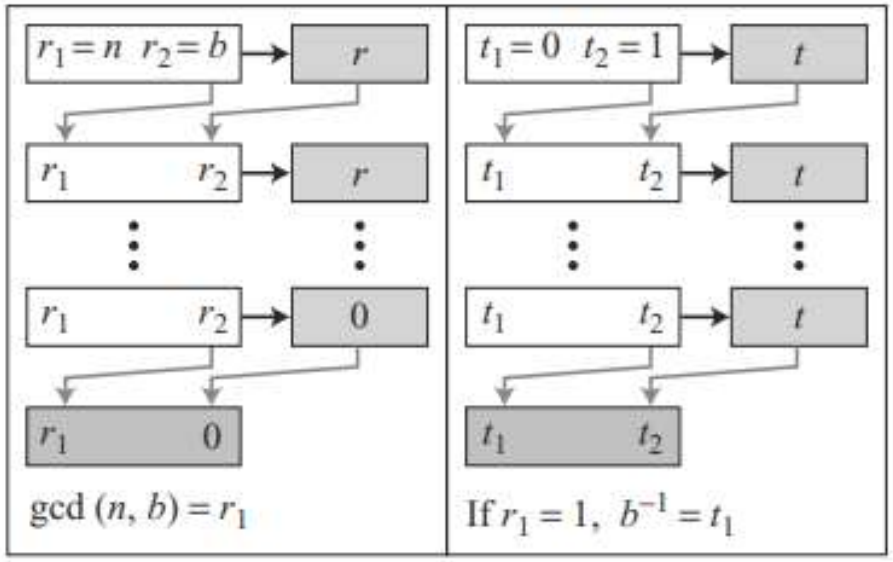
- In Z_{11}, gcd (11, a) is 1 (relatively prime) for all values of a except 0.
- It means all integers 1 to 10 have multiplicative .

The integer a in Z_n has a multiplicative inverse if and only if gcd $(n, a) \equiv 1 \pmod{n}$

Extended Euclidean algorithm and inverse

- The extended Euclidean algorithm finds the multiplicative inverses of b in Z_n when n and b are given and gcd (n, b) = 1.
- The multiplicative inverse of b is the value of t after being mapped to Z_n.

Extended Euclidean Algorithm to compute multiplicative inverse



a. Process

```
r1 ← n; r2 ← b;
t1 ← 0; t2 ← 1;
while (r2 > 0)
 {
  q ← r1 / r2;
  r ← r1 - q × r2;
  r1 ← r2;  r2 ← r;
  t ← t1 - q × t2;
  t1 ← t2;  t2 ← t;
 }
  if (r1 = 1) then b^-1 ← t1
```

b. Algorithm

Find multiplicative inverse using Extended Euclidean algorithm

Q=A/B	A	B	R= A % B	T1	T2	T= T1-Q*T2
				0	1	

A > B
Q=A/B
R= A%B
T1=0, T2 =1 T= T1-Q*T2

A=B
B=R
T1=T2
T2=T

Find the multiplicative inverse of 11 in Z26

Q=r1/r2	r1	r2	R	T1	T2	T=t1 − q × t2
2	26	11	4	0	1	-2
2	11	4	3	1	-2	5
1	4	3	1	-2	5	-7
3	3	1	0	5	-7	26
	1	0		-7	26	

GCD(26,11)=1, i.e. multiplicative inverse exists

Multiplicative inverse = T1= -7 = 26-7= **19**

Find the inverse of 12 in $\mathbf{Z_{26}}$.

Solution

We use a table similar to the one we used before, with $r_1 = 26$ and $r_2 = 12$.

q	r_1	r_2	r	t_1	t_2	t
2	26	12	2	0	1	−2
6	12	2	0	1	−2	13
	2	0		−2	13	

The gcd (26, 12) = 2 ≠ 1, which means there is no multiplicative inverse for 12 in $\mathbf{Z_{26}}$.

Find the multiplicative inverse of 23 in $\mathbf{Z}_{100}$.

Solution

We use a table similar to the one we used before with $r_1 = 100$ and $r_2 = 23$. We are interested only in the value of t.

q	r_1	r_2	r	t_1	t_2	t
4	100	23	8	0	1	−4
2	23	8	7	1	−4	19
1	8	7	1	−4	9	−13
7	7	1	0	9	−13	100
	1	0		−13	100	

The gcd (100, 23) is 1, which means the inverse of 23 exists. The extended Euclidean algorithm gives $t_1 = -13$. The inverse is $(-13) \bmod 100 = 87$. In other words, 13 and 87 are multiplicative inverses in $\mathbf{Z}_{100}$. We can see that $(23 \times 87) \bmod 100 = 2001 \bmod 100 = 1$.

Addition and Multiplication In cryptography

- If the sender uses an integer (as the encryption key), the receiver uses the inverse of that integer (as the decryption key).
- If the cryptographic operation is addition, Zn gives set of an additive inverse.
- if the operation is multiplication, Zn* gives multiplicative inverse

- Use Zn for additive inverses
- use Zn* when multiplicative inverses are needed.
- Z6 = {0, 1, 2, 3, 4, 5} Z6 * = {1, 5}
- Z7 = {0, 1, 2, 3, 4, 5, 6} Z7 * = {1, 2, 3, 4, 5, 6}
- Z10 = {0, 1, 2, 3, 4, 5, 6, 7, 8, 9} Z10* = {1, 3, 7, 9}

Zp and Zp* sets

- The modulus in Zp and Zp* sets is a prime number.
- a prime number has only two divisors: integer 1 and itself.
- The set Zp is the same as Zn except that n is a prime. i.e. Zp contains all integers from 0 to p − 1.
- Each member in Zp has an additive inverse;
- each member except 0 has a multiplicative inverse.

Zp and Zp* sets

- The set Zp* is the same as Zn* except that n is a prime.
- Zp* contains all integers from 1 to p − 1.
- Each member in Zp* has an additive and a multiplicative inverse.
- Zp* is a very good candidate when we need a set that supports both additive and multiplicative inverse.

Zp and Zp* set examples

- $Z_{13} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$
- $Z_{13}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$

MATRICES

- Representation in mathematics
- Rows and columns
- Addition, subtraction and multiplication operations

MATRICES

- Determinant:
  - a square matrix A of size m × m
  - denoted as det (A)
  - a scalar calculated recursively as :
    - 1. If m = 1, det (A) = a11
    - 2. If m > 1, det (A) = $\sum_{i=1}^{m}(-1)^{i+j} * a_{ij} \times \det(Aij)$

    Where Aij is a matrix obtained from A by deleting the ith row and jth column.
  - The determinant is defined only for a square matrix

Computing a determinant

- Formula: If m > 1, det (A) = $\sum_{i=1}^{m}(-1)^{i+j} * a_{ij} \times \det(A_{ij})$

$$\det\begin{bmatrix}5 & 2\\ 3 & 4\end{bmatrix} = (-1)^{1+1} \times 5 \times \det[4] + (-1)^{1+2} \times 2 \times \det[3] \longrightarrow 5 \times 4 - 2 \times 3 = 14$$

or $$\det\begin{bmatrix}a_{11} & a_{12}\\ a_{21} & a_{22}\end{bmatrix} = a_{11} \times a_{22} - a_{12} \times a_{21}$$

Computing a determinant

- Formula: If m > 1, det (A) = $\sum_{i=1}^{m}(-1)^{i+j} * a_{ij} \times \det(Aij)$

$$\det\begin{bmatrix} 5 & 2 & 1 \\ 3 & 0 & -4 \\ 2 & 1 & 6 \end{bmatrix} = (-1)^{1+1} \times 5 \times \det\begin{bmatrix} 0 & -4 \\ 1 & 6 \end{bmatrix} + (-1)^{1+2} \times 2 \times \det\begin{bmatrix} 3 & -4 \\ 2 & 6 \end{bmatrix} + (-1)^{1+3} \times 1 \times \det\begin{bmatrix} 3 & 0 \\ 2 & 1 \end{bmatrix}$$

$$= (+1) \times 5 \times (+4) \quad + \quad (-1) \times 2 \times (24) \quad + \quad (+1) \times 1 \times (3) = -25$$

Inverses of a matrix

- Matrices have both additive and multiplicative inverses.
- The additive inverse of matrix A is another matrix B such that A + B = 0.
- In other words, we have bij = − aij for all values of i and j.
- Normally the additive inverse of A is defined by −A

Multiplicative Inverse of a matrix

- The multiplicative inverse is defined only for square matrices.
- The multiplicative inverse of a square matrix A is a square matrix B such that $A \times B = B \times A = I$.
- multiplicative inverse of A is denoted as A^{-1}.
- The multiplicative inverse exists only if the det(A) has a multiplicative inverse in the corresponding set.
- Matrices with real elements have inverses only if det (A) $\neq 0$.

Residue Matrices

- residue matrices: matrices in which all elements are in Zn.
- All operations on residue matrices are performed the same as for the integer matrices but in modular arithmetic.
- A residue matrix has a multiplicative inverse if the determinant of the matrix has a multiplicative inverse in Zn.
- In other words, a residue matrix has a multiplicative inverse if gcd (det(A), n) = 1.

Example: Residue matrix and multiplicative inverse

A residue matrix and its multiplicative inverse

$$\mathbf{A} = \begin{bmatrix} 3 & 5 & 7 & 2 \\ 1 & 4 & 7 & 2 \\ 6 & 3 & 9 & 17 \\ 13 & 5 & 4 & 16 \end{bmatrix} \qquad \mathbf{A}^{-1} = \begin{bmatrix} 15 & 21 & 0 & 15 \\ 23 & 9 & 0 & 22 \\ 15 & 16 & 18 & 3 \\ 24 & 7 & 15 & 3 \end{bmatrix}$$

$$\det(\mathbf{A}) = 21 \qquad \det(\mathbf{A}^{-1}) = 5$$

- In Z_{26}

LINEAR CONGRUENCE

- Single variable linear equation.
- solving an equation or a set of equations of one or more variables with coefficient in Zn
- e.g. Assume equation: $ax \equiv b \pmod{n}$.
- This equation might have no solution or a limited number of solutions.
- If gcd (a, n) = d,
  - If $d \nmid b$, there is no solution.
  - If $d \mid b$, there are d solutions.

Applications of linear Congruence

- $10x = 2 \pmod{15}$
- $14x = 12 \pmod{18}$
- $3x+4=6 \pmod{13}$

- Can solve for more than one variable using matrices.

Cryptography

- Cryptography can reformat and transform our data, making it safer on its trip between computers. The technology is based on the essentials of secret codes, augmented by modern mathematics that protects our data in powerful ways.
- Computer Security - generic name for the collection of tools designed to protect data and to thwart hackers
- Network Security - measures to protect data during their transmission
- Internet Security - measures to protect data during their transmission over a collection of interconnected networks

Basic Concepts

- Cryptography The art or science encompassing the principles and methods of transforming an intelligible message into one that is unintelligible, and then retransforming that message back to its original form
- Plaintext The original intelligible message
- Cipher text The transformed message
- Cipher An algorithm for transforming an intelligible message into one that is unintelligible by transposition and/or substitution methods
- Key Some critical information used by the cipher, known only to the sender& receiver
- Encipher (encode) The process of converting plaintext to cipher text using a cipher and a key
- Decipher (decode) the process of converting cipher text back into plaintext using a cipher and a key.

- Cryptanalysis : The study of principles and methods of transforming an unintelligible message back into an intelligible message without knowledge of the key. Also called code breaking
- Cryptology Both cryptography and cryptanalysis
- Code An algorithm for transforming an intelligible message into an unintelligible one using a code-book

Categories of Cryptographic System

Characterized along three independent dimensions:

1. **The type of operations used for transforming plaintext to cipher text.**

2. **The number of keys used.**

3. **The way in which the plaintext is processed.**

Categories of Cryptographic System

The type of operations used for transforming plaintext to cipher text-

All encryption algorithms are based on two general principles:

- Substitution
- Transpositions

Categories of Cryptographic System

Substitution

- Each element in the plaintext (bit, letter, group of bits or letters) is mapped into another element

Transposition

- Elements in the plaintext are rearranged.

- The fundamental requirement is that no information be lost (i.e., that all operations are reversible).
- Most systems involve multiple stages of substitutions and transpositions.

Categories of Cryptographic System

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.**

Categories of Cryptographic System

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.

Classification of Cryptographic System

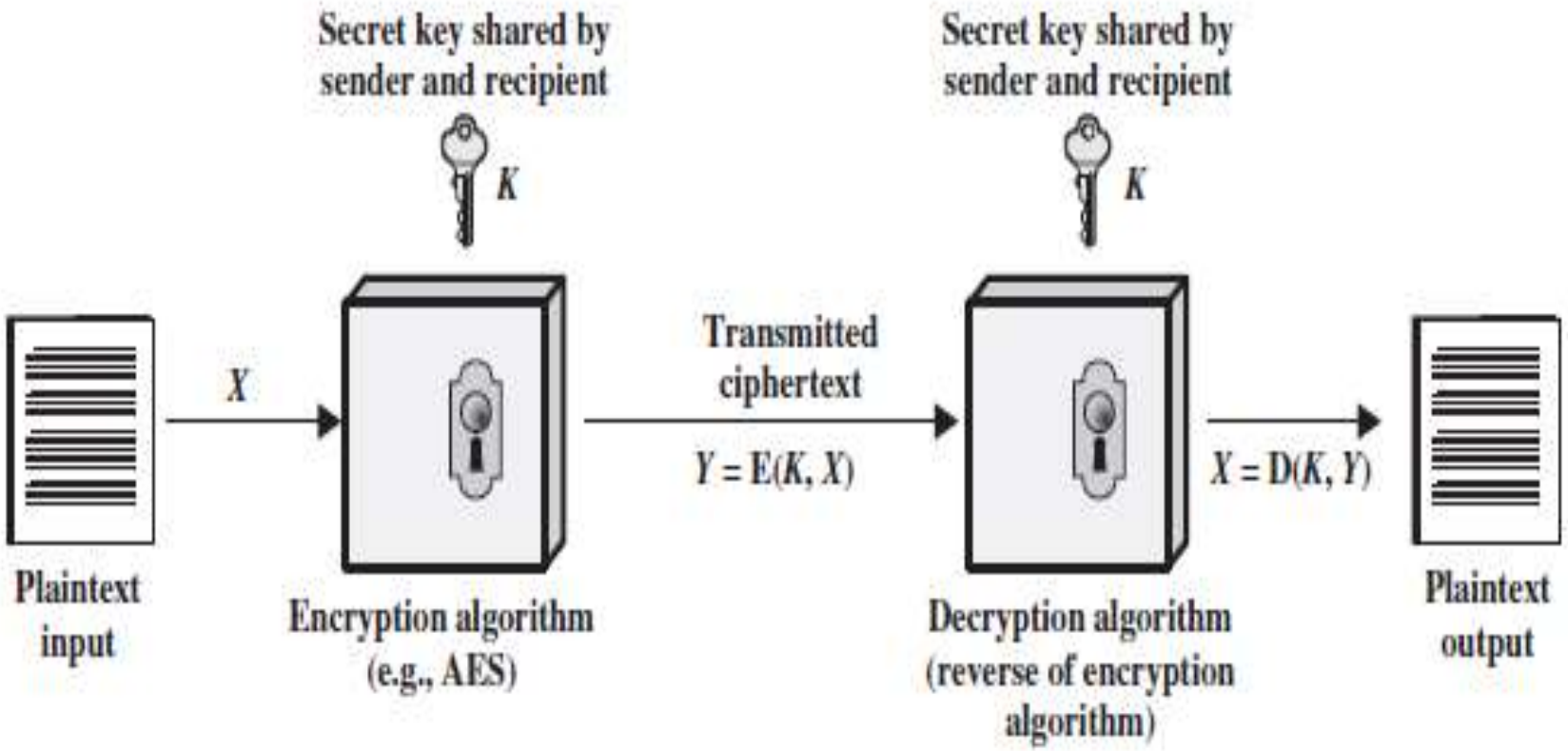
- Type of operations used for transforming plain text to cipher text
  - substitution, in which each element in the plaintext is mapped into another element, and
  - transposition, in which elements in the plaintext are rearranged.
- The number of keys used:
  - If the sender and receiver uses same key then it is said to be symmetric key (or) single key (or) conventional encryption.
  - If the sender and receiver use different keys then it is said to be public key encryption.
- The way in which the plain text is processed
  - A block cipher processes the input and block of elements at a time, producing output block for each input block.
  - A stream cipher processes the input elements continuously, producing output element one at a time, as it goes along.

Symmetric Encryption

A symmetric encryption scheme has five ingredients

- **Plaintext**
- **Encryption algorithm**
- **Secret key**
- **Ciphertext**
- **Decryption algorithm**

Symmetric Encryption



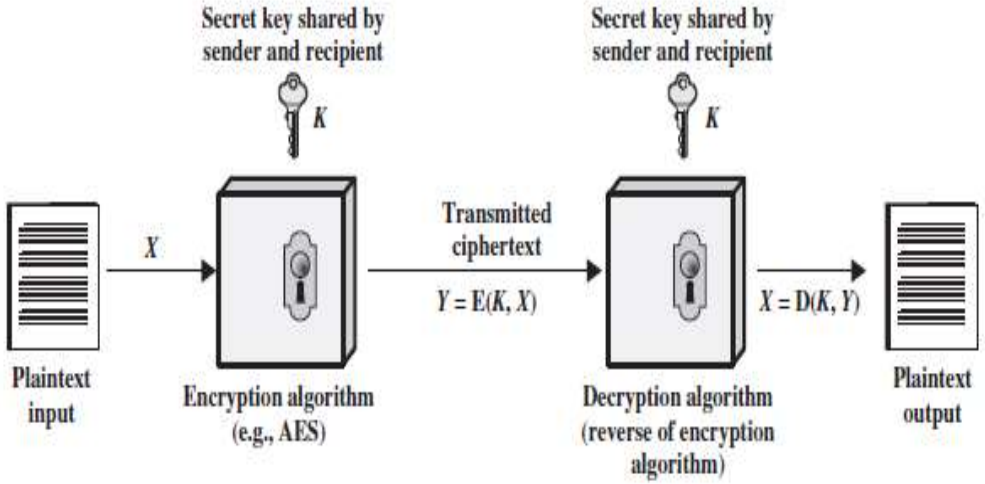
Symmetric Encryption

Plaintext

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

Encryption algorithm

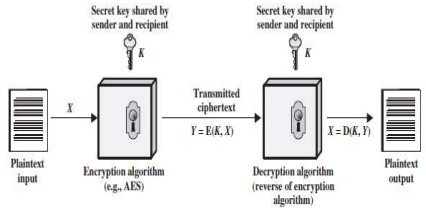
- The encryption algorithm performs various substitutions and transformations on the plaintext.



Symmetric Encryption

Secret key:

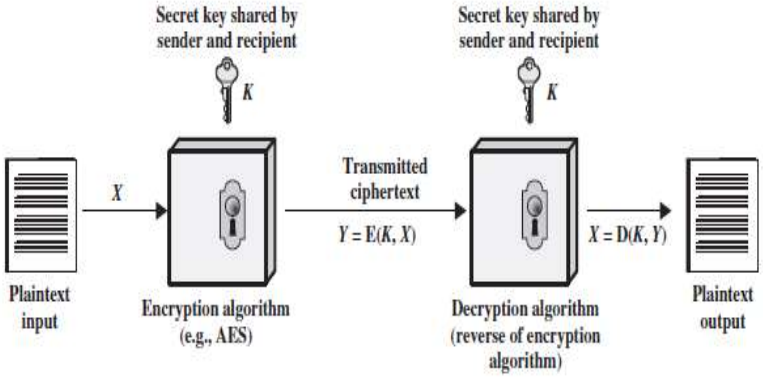
- The secret key is also input to the encryption algorithm.
- The key is a value independent of the plaintext and of the algorithm.
- The algorithm will produce a different output depending on the specific key being used at the time.
- The exact substitutions and transformations performed by the algorithm depend on the key.



Symmetric Encryption

Cipher text

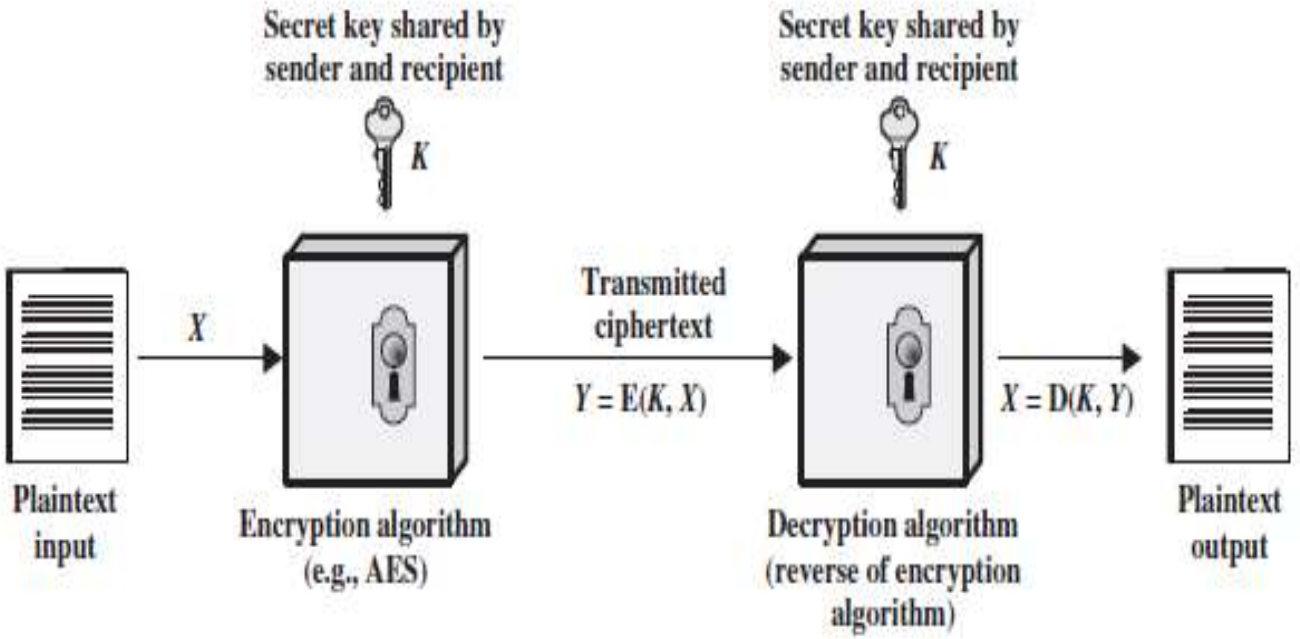
- This is the scrambled message produced as output.
- An apparently random stream of data and, as it stands, is unintelligible.
- It depends on the plaintext and the secret key.
- For a given message, two different keys will produce two different cipher texts.



Symmetric Encryption

Decryption algorithm

- This is essentially the encryption algorithm run in reverse.
- It takes the cipher text and the secret key and produces the original plaintext.



Symmetric Encryption

Requirements for secure use of conventional/Symmetric encryption:

- A strong encryption algorithm.
- Secure Secret Key

Symmetric Encryption

A strong encryption algorithm.

- Even if the opponent knows the algorithm and has access to one or more ciphertexts, Still would be unable to decipher the ciphertext or figure out the key.
- The opponent should be unable to decrypt ciphertext or discover the key even if he or she is in possession of a number of ciphertexts together with the plaintext that produced each ciphertext.

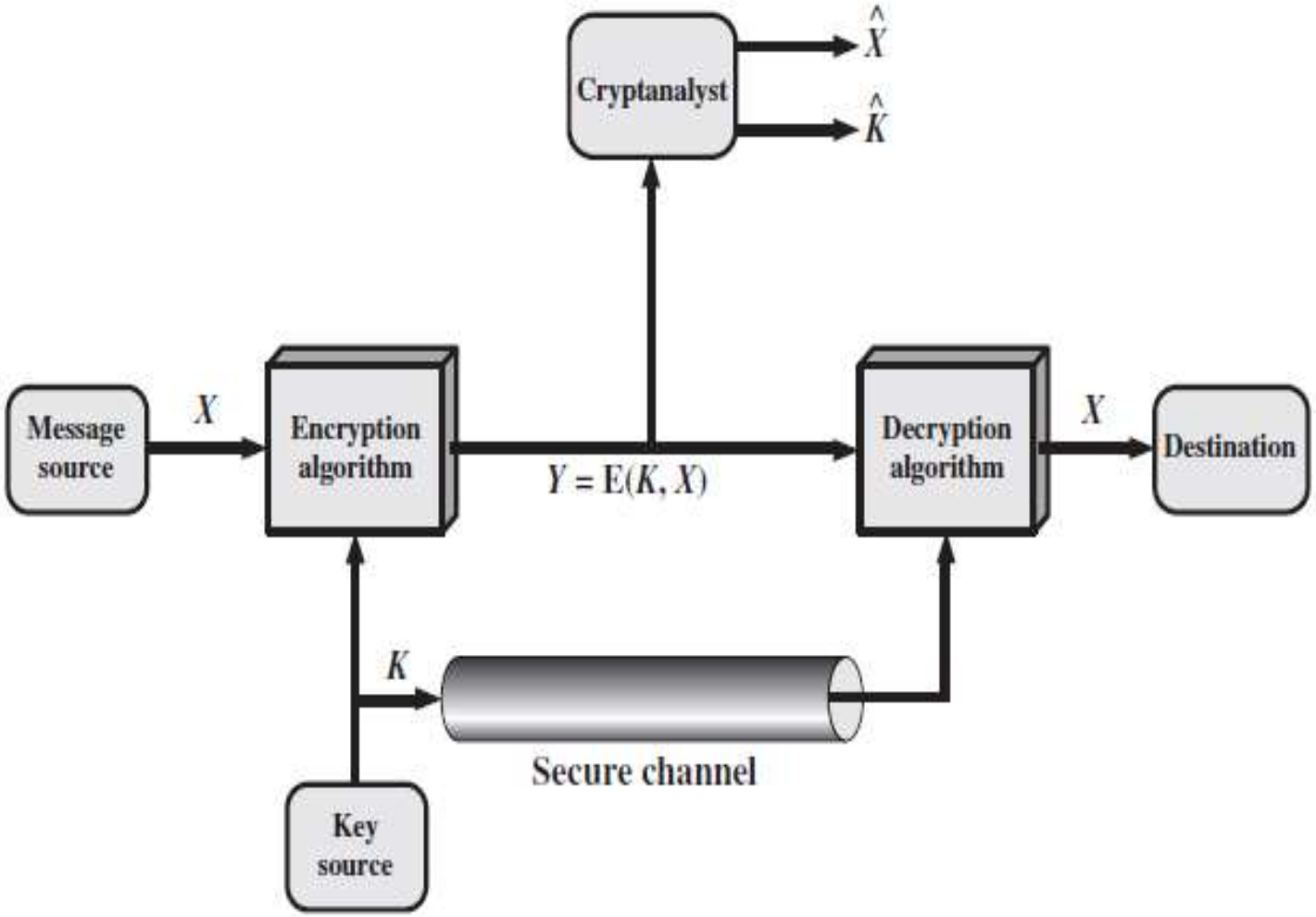
Symmetric Encryption

Secure Secret Key-

- Sender and receiver must have
  - obtained copies of the secret key in a secure fashion and
  - must keep the key secure.

- If someone can discover the key and knows the algorithm, all communication using this key is readable.

Model of Symmetric Cryptosystem



Model of Symmetric Cryptosystem

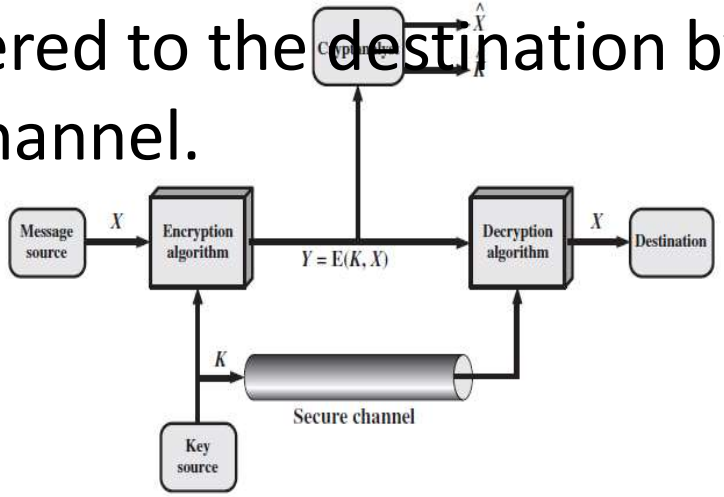
- A source produces a message in plaintext,

$$X = [X1, X2, \ldots\ldots\ldots, XM].$$

- The *M* elements of *X* are letters in some finite alphabet(26 Capital letters or {0,1})
- Key generation

$$K = [K1, K2, c, KJ]$$

- If the key is generated at the Message source or Third Party, delivered to the destination by means of some secure channel.



Model of Symmetric Cryptosystem

- Cipher text generation

$Y =$

$[Y1, Y2, \ldots\ldots, YN]$.

$Y =$

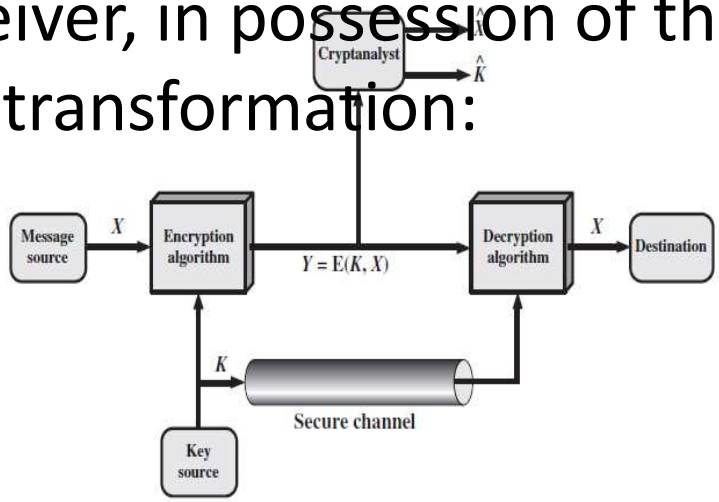
$E(K, X)$

- Y is produced by using encryption algorithm E as a function of the plaintext X, the value of the key K.

- The intended receiver, in possession of the key, is able to invert the transformation:

$X =$

$D(K, Y)$



Cryptanalysis

Cryptanalysis is the study and process of analyzing and decrypting ciphers, codes, and encrypted text without using the real key. Alternately, we can say it's the technique of accessing a communication's plain text content when you don't have access to the decryption key.

Put simply, cryptanalysis is the practice, science, or art of decrypting encrypted messages.

Cryptanalysis

- Cryptanalysis experts study ciphers, cryptosystems, and ciphertext to understand their functions.
- Then, they use that knowledge to find or improve techniques to weaken or defeat them.
- Cryptographer : one who writes encryption code used in cybersecurity,
- Cryptoanalyst : one who tries to crack those encryption codes.
- Two opposing sides of the cybersecurity coin, locked in conflict, trying to one-up the other, constantly inventing new measures and countermeasures.

Who Uses Cryptanalysis?

- Hackers use cryptanalysis.
- Would-be hackers use cryptanalysis to root out cryptosystem vulnerabilities rather than a brute force attack.
- Governments use cryptanalysis to decipher the encrypted messages of other nations.
- Companies specializing in cybersecurity products and services use cryptanalysis to test their security features.
- Even the world of academia gets in on the action, with researchers and academicians looking for weaknesses in cryptographic algorithms and protocols.
- Black-hat hackers use it to commit cybercrimes, and white-hat hackers use it to conduct penetration testing as directed by organizations that hire them to test their security.

Cryptanalysis Attacks and Techniques

1. Ciphertext-Only Attack

The attacker only has access to :

- at least one encrypted message
- but does not know the plaintext data, any cryptographic key data used, or the encryption algorithm being employed.
- Intelligence agencies often face this challenge when they've intercepted encrypted communications from a target.
- However, this is a formidable attack to pull off, thanks to the lack of target data.

Ciphertext-Only Attack (COA)

- **Problem:** cryptanalyze : **"DQG D FKLOG UHQWLQJ."**
  Assume the cipher is a Monoalphabetic substitution cipher. Decrypt the message.
- **Solution:**
- Since only the ciphertext is given, try all possible cipher shifts (brute force).
- Shifting letters by 3 (common Caesar cipher key):
  - 'D' → 'A', 'Q' → 'N', 'G' → 'D', etc.
- Decrypted text: **"AND A CHILD RENTING."**
- Success with a shift of 3.

Cryptanalysis Attacks and Techniques

2. Known Plaintext Attack

- This attack is easier to implement, compared to the ciphertext-only attack.
- analyst most likely has access to some or all the ciphertext’s plaintext.
- The goal is to discover the key the target uses to encrypt the message and use the key to decrypt the message.
- Once the key is discovered, the attacker can decrypt every message encrypted with that specific key.
- Known plaintext attacks rely on the attacker finding or guessing all or part of an encrypted message, or alternately, even the original plaintext's format.

Cryptanalysis Attacks and Techniques

3. Chosen Plaintext Attack

- Analysts using a chosen plaintext attack either already knows the encryption or can use the device used for encryption.
- The cryptanalyst can then encrypt the chosen plaintext using the targeted algorithm to gather information regarding the key.

Cryptanalysis Attacks and Techniques

4. A chosen-ciphertext attack

- cryptanalyst can analyse any chosen ciphertexts together with their corresponding plaintexts.
- the goal is to acquire a secret key or to get as many information about the attacked system as possible.
- The attacker has capability to make the victim (who obviously knows the secret key) decrypt any ciphertext and send him back the result.
- By analysing the chosen ciphertext and the corresponding received plaintext, the intruder tries to guess the secret key which has been used by the victim.
- Chosen-ciphertext attacks are usually used for breaking systems with public key encryption.
- For example, early versions of the RSA cipher were vulnerable to such attacks. They are used less often for attacking systems protected by symmetric ciphers. Some self-synchronizing stream ciphers have been also attacked successfully in that way.

Brute-Force Attack

Brute-force attack:

- Involves trying every possible key until an intelligible translation of the ciphertext into plaintext is obtained.

- On average, half of all possible keys must be tried to achieve success.

- That is, if there are *X* different keys, on average an attacker would discover the actual key after *X*/2 tries

- Statistical Attack:
- The cryptanalyst can benefit from some inherent characteristics of the plaintext language to launch a statistical attack.
- For example, we know that the letter E is the most frequently used letter in English text. The cryptanalyst finds the mostly used character in the ciphertext and assumes that the corresponding plaintext character is E. After finding a few pairs, the analyst can find the key and use it to decrypt the message.
- To prevent this type of attack, the cipher should hide the characteristics of the language.

- Pattern Attack :
- Some ciphers may hide the characteristics of the language, but may create some patterns in the ciphertext. A cryptanalyst may use a pattern attack to break the cipher. Therefore, it is important to use ciphers that make the ciphertext look as random as possible.

Cryptanalysis Tools

- **Cryptol:** This tool is an open-source license initially designed to be used by the Nation Security Agency (NSA), the United States intelligence agency, targeting cryptographic algorithms. Cryptol allows users to monitor how algorithms operate in programs that specify the ciphers or algorithms.
- **CrypTool:** CrypTool is another open-source offering that creates elearning programs, plus a web portal designed to help users learn about cryptographic algorithms and cryptanalysis.
- **Ganzua:** Ganzua is the Spanish term for a skeleton key or lockpick. It's an open-source, multi-platform Java-based tool that allows analysts to define almost totally arbitrary cipher and plain alphabets. In addition, this function will enable users to crack non-English cryptograms.

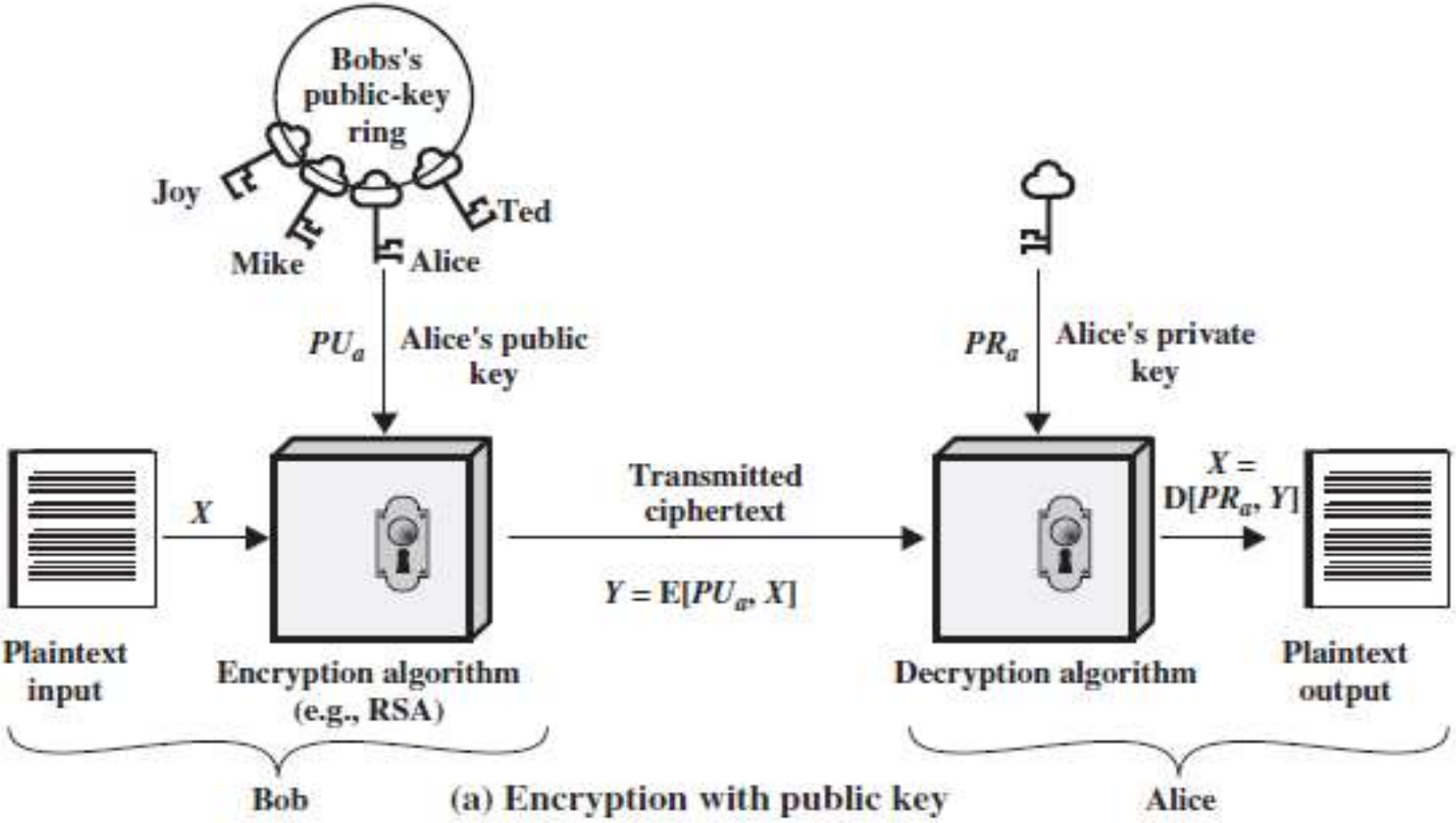
Kerckhoff's principle

- one should always assume that the adversary, Eve, knows the encryption/decryption algorithm.
- The resistance of the cipher to attack must be based only on the secrecy of the key.
- In other words, guessing the key should be so difficult that there is no need to hide the encryption /decryption algorithm.
- There are only a few algorithms for modern ciphers today.
- The key domain for each algorithm, however, is so large that it makes it difficult for the adversary to find the key.

Asymmetric cryptography

- Public-key cryptography
- Asymmetric cryptography,
- A cryptographic system that uses pairs of keys
- Public keys (which may be known to others),
- Private keys (which may never be known by any except the owner).

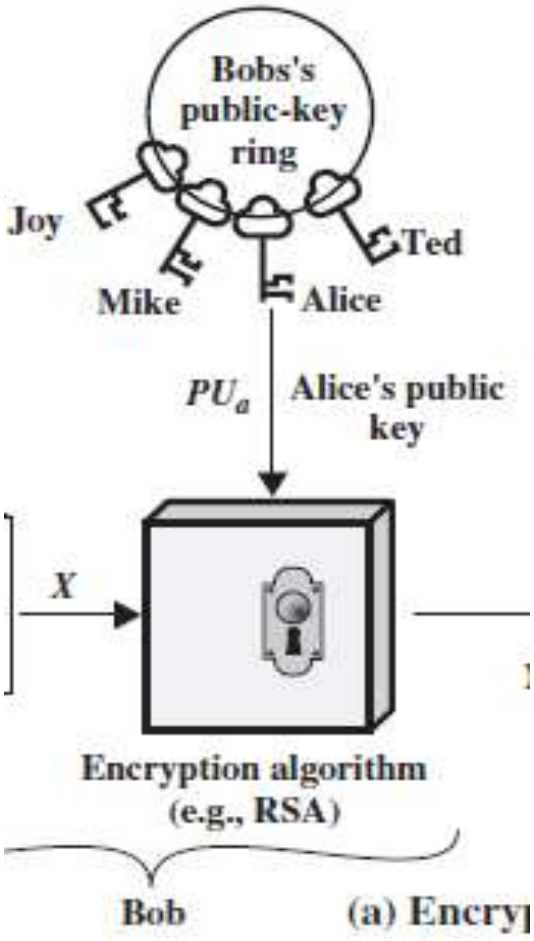
Asymmetric cryptography



Asymmetric cryptography

The essential steps are the following.

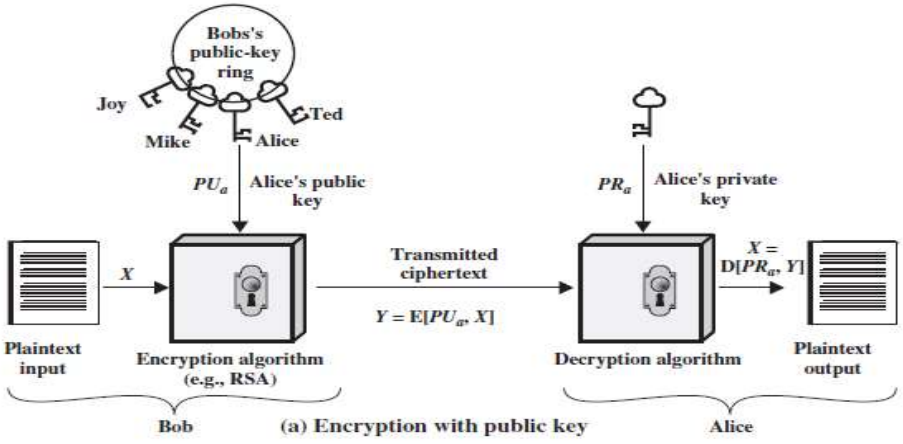
- Each user generates a pair of keys to be used for the encryption and decryption of messages.
- Each user places one of the two keys in a public register or other accessible file. This is the public key.
- The companion key is kept private.
- Each user maintains a collection of public keys obtained from others.



Asymmetric cryptography

The essential steps are the following.

- If Bob wishes to send a confidential message to Alice
- Bob encrypts the message using Alice's public key.
- 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.



Difference between Symmetric and Asymmetric Encryption

Symmetric Key Encryption	Asymmetric Key Encryption
It only requires a single key for both encryption and decryption.	It requires two key one to encrypt and the other one to decrypt.
The size of cipher text is same or smaller than the original plain text.	The size of cipher text is same or larger than the original plain text.
The encryption process is very fast.	The encryption process is slow.
It is used when a large amount of data is required to transfer.	It is used to transfer small amount of data.
It only provides confidentiality.	It provides confidentiality, authenticity and non-repudiation.
Examples: 3DES, AES, DES and RC4	Examples: Diffie-Hellman, ECC, El Gamal, DSA and RSA
In symmetric key encryption, resource utilization is low as compared to asymmetric key encryption.	In asymmetric key encryption, resource utilization is high.

Classical Encryption Techniques

- **Substitution**
  - **Transposition**

Substitution

- **One in which the letters of plaintext are replaced by other letters or by numbers or symbols.**
- **If the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with ciphertext bit patterns.**

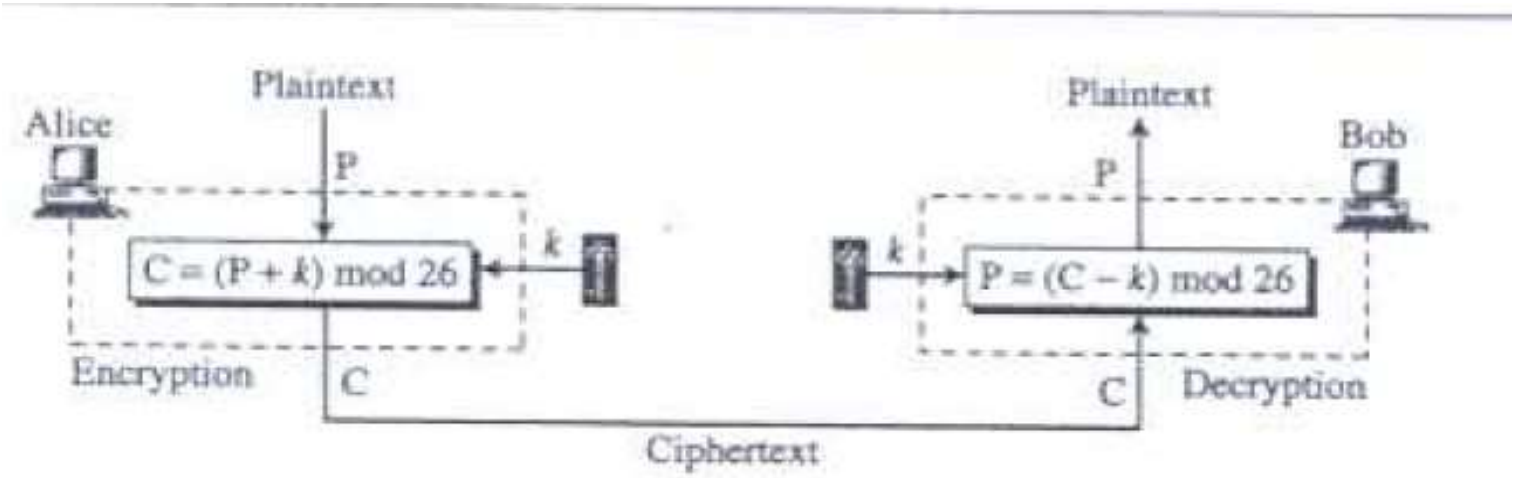
Substitution Cipher

- MONOALPHABETIC CIPHER
  - Aditive (Shift / Ceasar)
  - Multiplicative
  - Affine

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,**

Additive (Shift / Ceasar)



- Cryptanalysis
- Easy to decode
- Prone to statistical attack
- Sometimes use digram trigram.

Caesar Cipher

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
```

Caesar Cipher

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:
- $C = E(3, p) = (p + 3) \bmod 26$

Caesar Cipher

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

$$C = E(k, p) = (p + k) \bmod 26$$

- where k takes on a value in the range 1 to 25.

- The decryption algorithm is simply

$$p = D(k, C) = (C - k) \bmod 26$$

- If it is known that a given cipher text is a Caesar cipher, then a brute-force cryptanalysis is easily performed: simply try all the 25 possible keys.

Brute-Force Cryptanalysis of Caesar Cipher

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

KEY	PHHW PH DIWHU WKH WRJD SDUWB
1	oggv og chvgt vjg vqic rctva
2	nffu nf bgufs uif uphb qbsuz
3	meet me after the toga party
4	ldds ld zesdq sgd snfz ozqsx
5	kccr kc ydrcp rfc rmey nyprw
6	jbbq jb xcqbo qeb qldx mxoqv
7	iaap ia wbpan pda pkcw lwnpu
8	hzzo hz vaozm ocz ojbv kvmot
9	gyyn gy uznyl nby niau julns
10	fxxm fx tymxk max mhzt itkmr
11	ewwl ew sxlwj lzw lgys hsjlq
12	dvvk dv rwkvi kyv kfxr grikp
13	cuuj cu qvjuh jxu jewq fqhjo
14	btti bt puitg iwt idvp epgin
15	assh as othsf hvs hcuo dofhm
16	zrrg zr nsgre gur gbtn cnegl
17	yqqf yq mrfqd ftq fasm bmdfk
18	xppe xp lqepc esp ezrl alcej
19	wood wo kpdob dro dyqk zkbdi
20	vnnc vn jocna cqn cxpj yjach
21	ummb um inbmz bpm bwoi xizbg
22	tlla tl hmaly aol avnh whyaf
23	skkz sk glzkx znk zumg vgxze
24	rjjy rj fkyjw ymj ytlf ufwyd
25	qiix qi ejxiv xli xske tevxc

Brute-Force Cryptanalysis of Caesar Cipher

Caesar Cipher

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

$$C = E(k, p) = (p + k) \bmod 26$$

- where k takes on a value in the range 1 to 25.

- The decryption algorithm is simply

$$p = D(k, C) = (C - k) \bmod 26$$

- If it is known that a given cipher text is a Caesar cipher, then a brute-force cryptanalysis is easily performed: simply try all the 25 possible keys.

Caesar Cipher

- With only 25 possible keys, the Caesar cipher is far from secure.
- A dramatic increase in the key space can be achieved by allowing an arbitrary substitution.
- Permutation!!

Caesar Cipher

- A **permutation** of a finite set of elements *S* is an ordered sequence of all the elements of *S*, with each element appearing exactly once.

- For example,

S = {a, b, c}, there are six permutations of *S*:
abc, acb, bac, bca, cab, cba

- There are *n*! permutations of a set of *n* elements,
  - The first element can be chosen in one of *n* ways,
  - The second in *n* - 1 ways,
  - The third in *n* – 2 ways, and so on.

Caesar Cipher

- Caesar Cipher-

```
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
```

- If, instead, the “cipher” line can be any permutation of the 26 alphabetic characters, then there are 26! possible keys.

- Such an approach is referred to as a monoalphabetic substitution cipher, because a single cipher alphabet (mapping from plain alphabet to cipher alphabet) is used per message.

Monoalphabetic Cipher

- Monoalphabetic cipher is one where each character of a plain text is mapped to a fixed other character of cipher text.

- Examples of monoalphabetic ciphers would include the Caesar-shift cipher,

Monoalphabetic Cipher-Example

- The ciphertext to be solved is

```
UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ
```

- As a first step, the relative frequency of the letters can be determined

P 13.33	H 5.83	F 3.33	B 1.67	C 0.00
Z 11.67	D 5.00	W 3.33	G 1.67	K 0.00
S 8.33	E 5.00	Q 2.50	Y 1.67	L 0.00
U 8.33	V 4.17	T 2.50	I 0.83	N 0.00
O 7.50	X 4.17	A 1.67	J 0.83	R 0.00
M 6.67				

Monoalphabetic Cipher

- The relative frequency of the letters can be compared to a standard frequency distribution for English

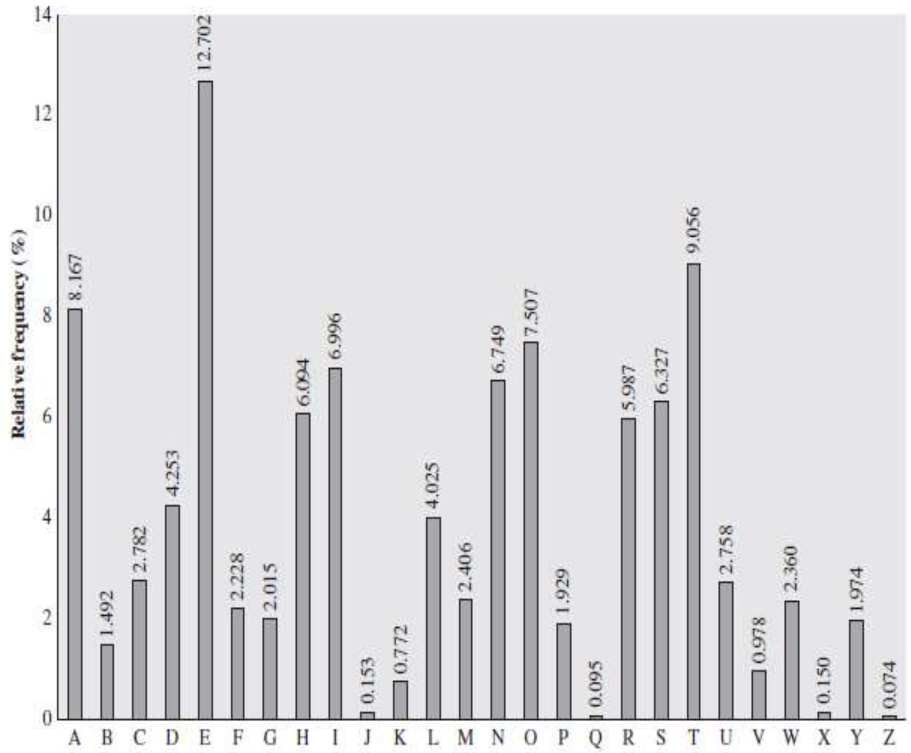
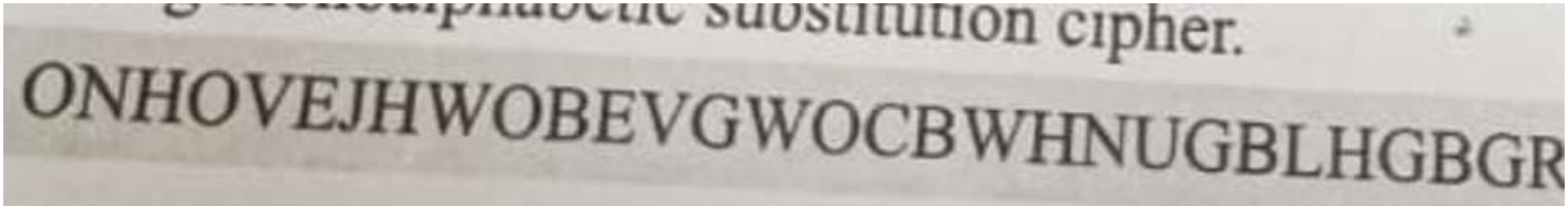


Figure 2.5 Relative Frequency of Letters in English Text



Monoalphabetic Cipher

Comparison-

- Cipher letters P and Z are the equivalents of plain letters e and t, but it is not certain which is which.
- The letters S, U, O, M, and H are all of relatively high frequency and probably correspond to plain letters from the set {a, h, i, n, o, r, s}.
- The letters with the lowest frequencies (namely, A, B, G, Y, I, J) are likely included in the set {b, j, k, q, v, x, z}.

Monoalphabetic Cipher

- We could make some tentative assignments and start to fill in the plaintext to see if it looks like a reasonable “skeleton” of a message.

- A more systematic approach is to look for other regularities.
  - For example, certain words may be known to be in the text.
  - Or we could look for repeating sequences of cipher letters and try to deduce their plaintext equivalents.

Monoalphabetic Cipher

- A powerful tool is to look at the frequency of two-letter combinations, known as **digrams**.
- The most common such digram is th.
  - In our ciphertext, the most common digram is ZW, which appears three times.
  - So we make the correspondence of Z with t and W with h.

- By our earlier hypothesis, we can equate P with e.
- The sequence ZWP appears in the ciphertext, thus equal to “the.”
- This is the most frequent trigram (three-letter combination) in English, which seems to indicate that we are on the right track.

Monoalphabetic Cipher

- Next, notice the sequence ZWSZ in the first line.
- We do not know that these four letters form a complete word, but if they do, it is of the form th_t.
- If so, S equates with a

```
UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ
```

Monoalphabetic Cipher

- So far, then, we have Only four letters have been identified, but already we have quite a bit of the messa

```
UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
 t a        e  e te  a that e e a       a
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
  e t   ta t ha e ee  a e  th    t  a
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ
 e  e e tat  e   the   t
```

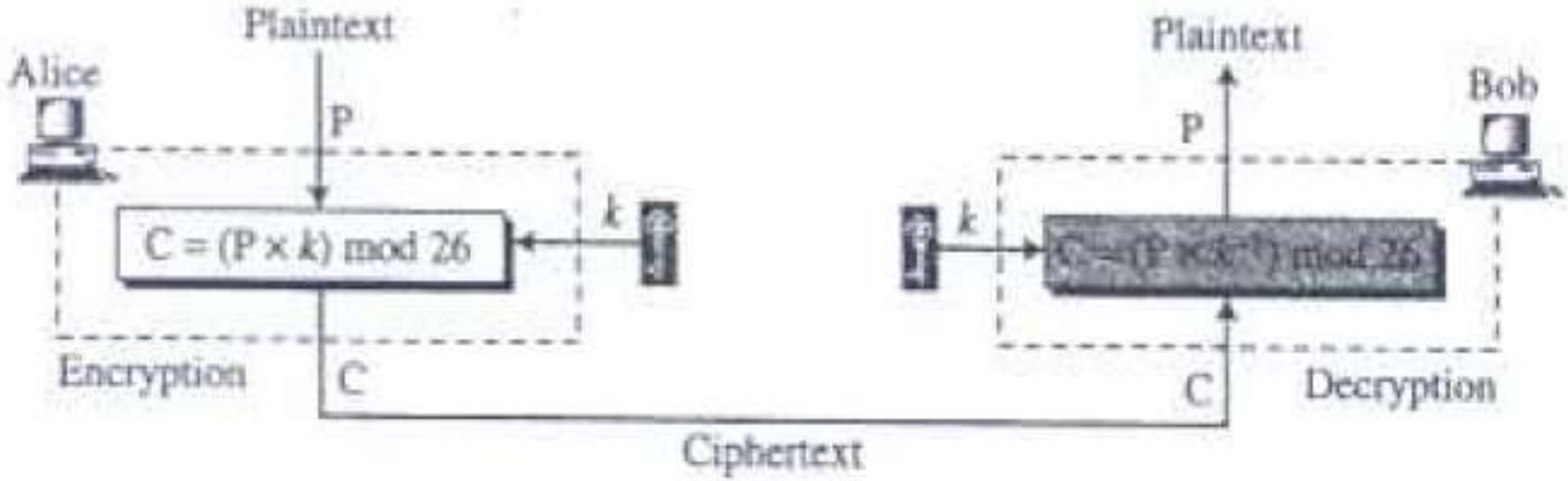
- Continued analysis of frequencies plus trial and error should easily yield a solution from this point

Monoalphabetic Cipher

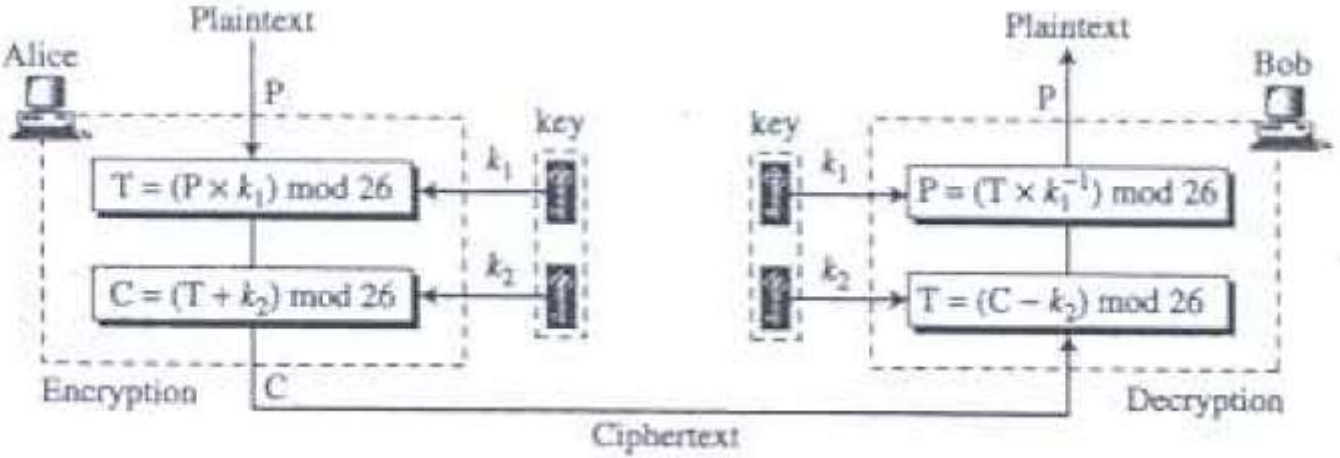
- The complete plaintext, with spaces added between words:

```
it was disclosed yesterday that several informal but
direct contacts have been made with political
representatives of the viet cong in moscow
```

Multiplicative



Affine



P: h → 07	Encryption: (07 × 7 + 2) mod 26	C: 25 → Z
P: e → 04	Encryption: (04 × 7 + 2) mod 26	C: 04 → E
P: l → 11	Encryption: (11 × 7 + 2) mod 26	C: 01 → B
P: l → 11	Encryption: (11 × 7 + 2) mod 26	C: 01 → B
P: o → 14	Encryption: (14 × 7 + 2) mod 26	C: 22 → W

C: Z → 25	Decryption: ((25 − 2) × 7^{-1}) mod 26	P:07 → h
C: E → 04	Decryption: ((04 − 2) × 7^{-1}) mod 26	P:04 → e
C: B → 01	Decryption: ((01 − 2) × 7^{-1}) mod 26	P:11 → l
C: B → 01	Decryption: ((01 − 2) × 7^{-1}) mod 26	P:11 → l
C: W → 22	Decryption: ((22 − 2) × 7^{-1}) mod 26	P:14 → o

Polyalphabetic Cipher

- A **polyalphabetic cipher** is a substitution, using multiple substitution alphabets
- One to many
- Hiding occurences
- Key stream k = {k1,k2,k3,.....}

Autokey Cipher

- The key is a stream of subkeys, in which each subkey is used to encrypt the corresponding character in the plaintext.
- The first subkey is a predetermined value secretly agreed upon by Alice and Bob.
- The second subkey is the value of the first plaintext character (between 0 and 25).
- The third subkey is the value of the second plaintext.
- And so on.

$P = P_1 P_2 P_3 \ldots$ $C = C_1 C_2 C_3 \ldots$ $k = (k_1, P_1, P_2, \ldots)$

Encryption: $C_i = (P_i + k_i) \bmod 26$ Decryption: $P_i = (C_i - k_i) \bmod 26$

Plaintext:	a	t	t	a	c	k	i	s	t	o	d	a	y
P's Values:	00	19	19	00	02	10	08	18	19	14	03	00	24
Key stream:	*12*	*00*	*19*	*19*	*00*	*02*	*10*	*08*	*18*	*19*	*14*	*03*	*00*
C's Values:	12	19	12	19	02	12	18	00	11	7	17	03	24
Ciphertext:	**M**	**T**	**M**	**T**	**C**	**M**	**S**	**A**	**L**	**H**	**R**	**D**	**Y**

Cryptanalysis of Autokey

- Hide single letter frequency
- Vulnerable to brute force attack as uses additive cipher

Playfair Cipher

- Playfair, treats **digrams** in the plaintext as single units
- Translates these units into ciphertext digrams

- The Playfair algorithm is based on the use of a 5 * 5 matrix of letters constructed using a keyword.

- In this case, the keyword is monarchy

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

Playfair Cipher

- The matrix is constructed by filling in the letters of the keyword (minus duplicates) from left to right and from top to bottom, and then filling in the remainder of the matrix with the remaining letters in alphabetic order.

- The letters I and J count as one letter.

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

Playfair Cipher

Plaintext is encrypted two letters at a time, according to the following rules:

1) Repeating plaintext letters that are in the same pair are separated with a filler letter, such as x, so that balloon would be treated as ba lx lo on.

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

Playfair Cipher

Plaintext is encrypted two letters at a time, according to the following rules:

1) Two plaintext letters that fall in the same row of the matrix are each replaced by the letter to the right, with the first element of the row circularly following the last.

For example, ar is encrypted as RM, st=TL

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

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

Playfair Cipher

Plaintext is encrypted two letters at a time, according to the following rules:

2. Two plaintext letters that fall in the same column are each replaced by the letter beneath, with the top element of the column circularly following the last.
For example, mu is encrypted as CM, me=CL

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

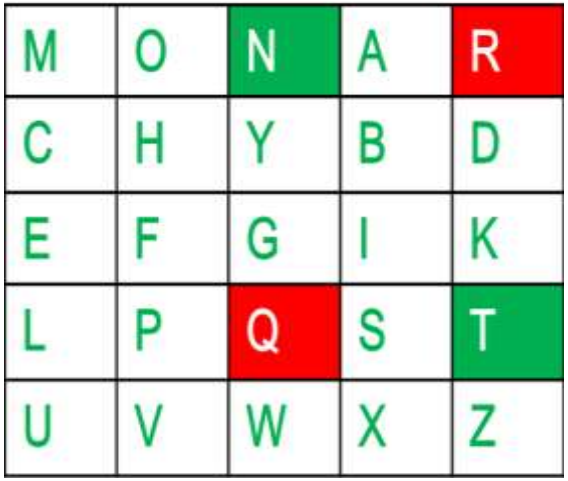
M	O	N	A	R
C	H	Y	B	D
E	F	G	I	K
L	P	Q	S	T
U	V	W	X	Z

Playfair Cipher

3. Otherwise, each plaintext letter in a pair is replaced by the letter that lies in its own row and the column occupied by the other plaintext letter. Thus, hs becomes BP and ea becomes IM (or JM, as the encipherer wishes).

Diagraph: "nt" **Encrypted Text:** rq

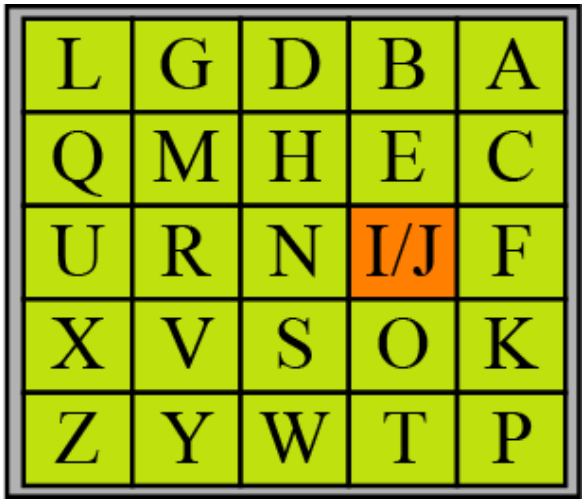
M	O	N	A	R
C	H	Y	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z



Playfair Cipher

Figure An example of a secret key matrix in the Playfair cipher

Secret Key =



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

Example

Let us encrypt the plaintext "hello" using the key in given Figure

he → EC lx → QZ lo → BX

Plaintext: hello Ciphertext: ECQZBX

Cryptanalysis of Playfair Cipher

- Brute force is difficult
- Size of key domain 25!
- Hides single letter frequency of characters
- Still leaves much of the structure of the plaintext language intact.
- A few hundred letters of ciphertext are generally sufficient
- Cryptanalyst can have ciphertext only attack based on digram frequency test to find the key

Polyalphabetic Cipher-Vignere Cipher

key: *deceptivedeceptivedeceptive*

plaintext: wearediscoveredsaveyourself

ciphertext: ZICVTWQNGRZGVTWAVZHCQYGLMGJ

Expressed numerically, we have the following result.

key	3	4	2	4	15	19	8	21	4	3	4	2	4	15
plaintext	22	4	0	17	4	3	8	18	2	14	21	4	17	4
ciphertext	25	8	2	21	19	22	16	13	6	17	25	6	21	19

key	19	8	21	4	3	4	2	4	15	19	8	21	4
plaintext	3	18	0	21	4	24	14	20	17	18	4	11	5
ciphertext	22	0	21	25	7	2	16	24	6	11	12	6	9

Strengths of Vignere Cipher

- There are multiple ciphertext letters for each plaintext letter, one for each unique letter of the keyword.
- Thus, the letter frequency information is obscured.
- However, not all knowledge of the plaintext structure is lost..

Polyalphabetic Cipher-Vignere Cipher

- Thus, the letter frequency information is obscured. However, not all knowledge of the plaintext structure is lost..

```
key:          deceptivedeceptivedeceptive
plaintext:    wearediscoveredsaveyourself
ciphertext:   ZICVTWQNGRZGVTWAVZHCQYGLMGJ
```

Expressed numerically, we have the following result.

key	3	4	2	4	15	19	8	21	4	3	4	2	4	15
plaintext	22	4	0	17	4	3	8	18	2	14	21	4	17	4
ciphertext	25	8	2	21	19	22	16	13	6	17	25	6	21	19

key	19	8	21	4	3	4	2	4	15	19	8	21	4
plaintext	3	18	0	21	4	24	14	20	17	18	4	11	5
ciphertext	22	0	21	25	7	2	16	24	6	11	12	6	9

Polyalphabetic Cipher-Vignere Cipher

- Plaintext letters P = p0, p1, p2, ……., pn-1
- A key consisting of the sequence of letters K = k0, k1, k2, ……., km-1,

where typically m < n

- Ciphertext letters C = C0, C1, C2, ……., Cn-1

$$C = C_0, C_1, C_2, \ldots, C_{n-1} = \mathrm{E}(K, P) = \mathrm{E}[(k_0, k_1, k_2, \ldots, k_{m-1}), (p_0, p_1, p_2, \ldots, p_{n-1})]$$
$$= (p_0 + k_0) \bmod 26, (p_1 + k_1) \bmod 26, \ldots, (p_{m-1} + k_{m-1}) \bmod 26,$$
$$(p_m + k_0) \bmod 26, (p_{m+1} + k_1) \bmod 26, \ldots, (p_{2m-1} + k_{m-1}) \bmod 26, \ldots$$

Polyalphabetic Cipher-Vignere Cipher

- Encryption Algorithm:

$$C_i = (p_i + k_{i \bmod m}) \bmod 26$$

- Decryption Algorithm:

$$p_i = (C_i - k_{i \bmod m}) \bmod 26$$

Polyalphabetic Cipher-Vignere Cipher

Example

Encrypt the message "She is listening" using the 6-character keyword "PASCAL".

Polyalphabetic Cipher-Vignere Cipher

Example

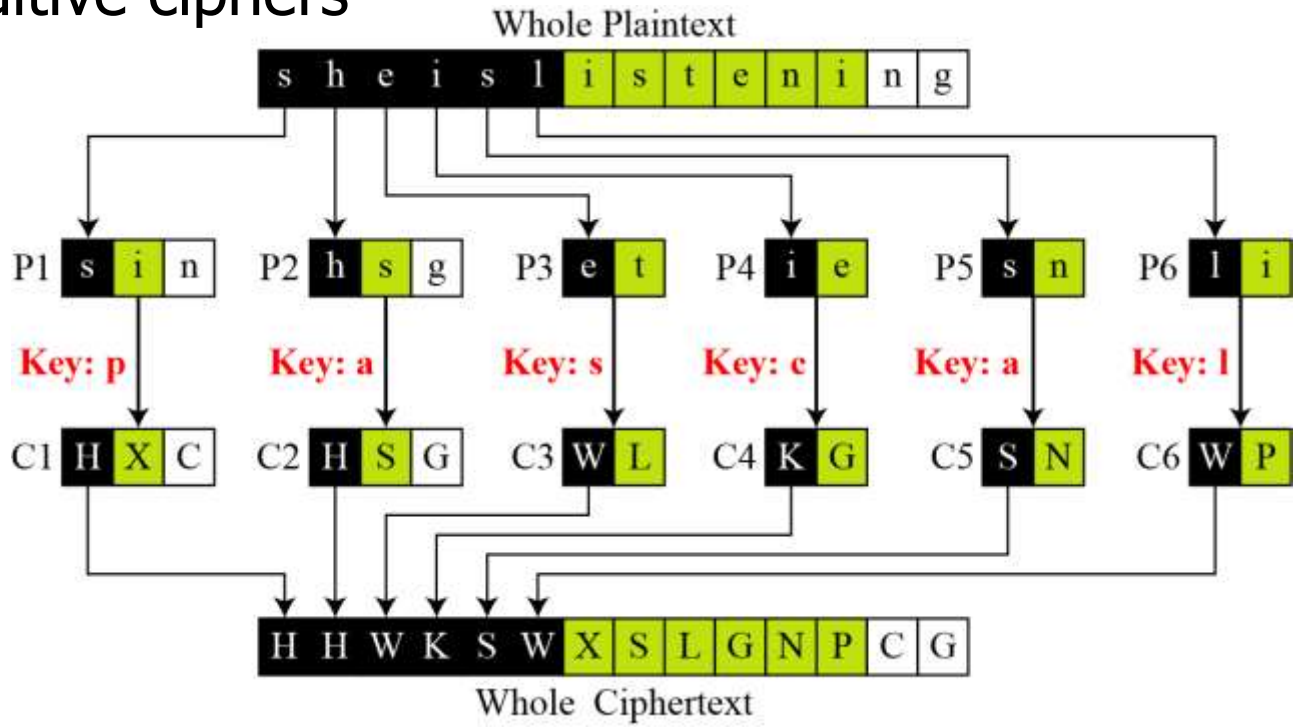
Let us see how we can encrypt the message "She is listening" using the 6-character keyword "PASCAL". The initial key stream is (15, 0, 18, 2, 0, 11). The key stream is the repetition of this initial key stream (as many times as needed).

Plaintext:	s	h	e	i	s	l	i	s	t	e	n	i	n	g
P's values:	18	07	04	08	18	11	08	18	19	04	13	08	13	06
Key stream:	*15*	*00*	*18*	*02*	*00*	*11*	*15*	*00*	*18*	*02*	*00*	*11*	*15*	*00*
C's values:	07	07	22	10	18	22	23	18	11	6	13	19	02	06
Ciphertext:	H	H	W	K	S	W	X	S	L	G	N	T	C	G

Example

Vigenere cipher can be seen as combinations of m additive ciphers.

Figure A Vigenere cipher as a combination of m additive ciphers



Vigenere Cipher (Cryptanalysis)

- Does not preserve frequency of characters
- cryptanalysis will be based on finding length of the key and finding key itself
- The Kasiski test for repetition of three-character segments yields the results
  - If two of these segments are found at distance d, the analyst assumes d/m where m is the key length
  - If more of repeated segments are found with distances d1,d2,..dn then gcd(d1,d2,..dn)/m
  - Segment of three letters avoids cases where characters in key are not distinct

Vigenere Cipher (Cryptanalysis)

Example

Let us assume we have intercepted the following ciphertext:

LIOMWGFEGGDVWGHHCQUCRHRWAGWIOWQLKGZETKKMEVLWPCZVGTH-
VTSGXQOVGCSVETQLTJSUMVWVEUVLXEWSLGFZMVVWLGYHCUSWXQH-
KVGSHEEVFLCFDGVSUMPHKIRZDMPHHBVWVWJWIXGFWLTSHGJOUEEHH-
VUCFVGOWICQLTJSUXGLW

The Kasiski test for repetition of three-character segments yields the results shown in Table

Table 3.4 *Kasiski test for Example 3.19*

String	*First Index*	*Second Index*	*Difference*
JSU	68	168	100
SUM	69	117	48
VWV	72	132	60
MPH	119	127	8

Example

The greatest common divisor of differences is 4, which means that the key length is multiple of 4. First try m = 4.

```
C1: LWGWCRAOKTEPGTQCTJVUEGVGUQGECVPRPVJGTJEUGCJG
P1: jueuapymircneroarhtsthihytrahcieixsthcarrehe
C2: IGGGQHGWGKVCTSOSQSWVWFVYSHSVFSHZHWWFSOHCOQSL
P2: usssctsiswhofeaeceihcetesoecatnpntherhctecex
C3: OFDHURWQZKLZHGVVLUVLSZWHWKHFDUKDHVIWHUHFWLUW
P3: lcaerotnwhiwedssirsiirhketehretltiideatrairt
C4: MEVHCWILEMWVVXGETMEXLMLCXVELGMIMBWXLGEVVITX
P4: iardysehaisrrtcapiafpwtethecarhaesfterectpt
```

In this case, the plaintext makes sense.

Julius Caesar used a cryptosystem in his wars, which is now referred to as Caesar cipher. It is an additive cipher with the key set to three. Each character in the plaintext is shifted three characters to create ciphertext.

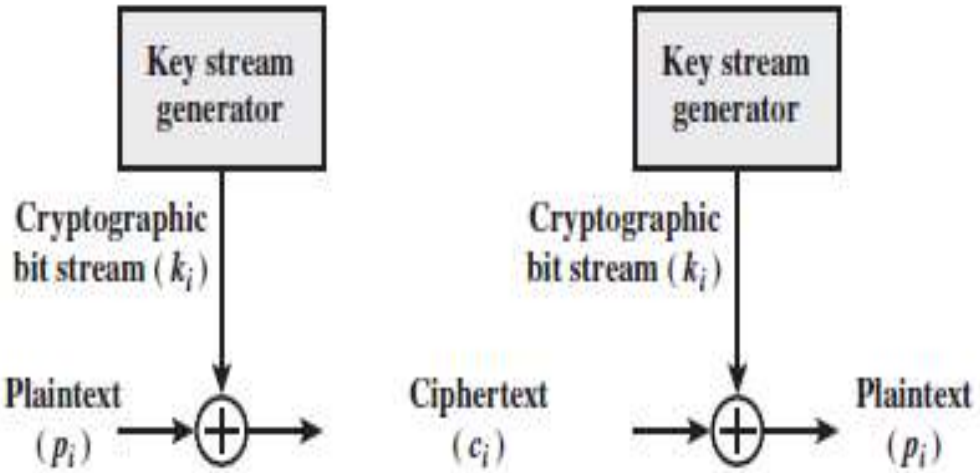
Vernam Cipher

- The ultimate defense against cryptanalysis
- To choose a keyword that is as long as the plaintext and has no statistical relationship to it.
- Such a system was introduced by an AT&T engineer named Gilbert Vernam in 1918.

Vernam Cipher

- It works on binary data (bits) rather than letters.
- The system can be expressed as :

$$c_i = p_i \oplus k_i$$



where

- p_i = *i*th binary digit of plaintext
- k_i = *i*th binary digit of key
- c_i = *i*th binary digit of ciphertext
- $\oplus$ = exclusive-or (XOR) operation

Vernam Cipher

- Ciphertext is generated by performing the bitwise XOR of the plaintext and the key.
- Because of the properties of the XOR, decryption simply involves the same bitwise operation:

$$p_i = c_i \oplus k_i$$

Vernam Cipher

- The essence of this technique is the means of construction of the key.

- Vernam proposed the use of a running loop of tape that eventually repeated the key, So the system worked with a very long but repeating keyword.

- Although such a scheme, with a long key, presents formidable cryptanalytic difficulties,
- It can be still broken with sufficient ciphertext, the use of known or probable plaintext sequences, or both.

The Hill Algorithm

- This encryption algorithm
  - Takes m successive plaintext letters
  - Substitutes for them m ciphertext letters.
  - Substitution determined by m linear equations
  - Each character is assigned a numerical value (a = 0, b = 1, c, z = 25)

The Hill Algorithm

- For m = 3, the system can be described as

$$c_1 = (k_{11}p_1 + k_{21}p_2 + k_{31}p_3) \bmod 26$$
$$c_2 = (k_{12}p_1 + k_{22}p_2 + k_{32}p_3) \bmod 26$$
$$c_3 = (k_{13}p_1 + k_{23}p_2 + k_{33}p_3) \bmod 26$$

- This can be expressed in terms of row vectors and matrices:

$$(c_1\ c_2\ c_3) = (p_1\ p_2\ p_3)\begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix} \bmod 26$$

$$\mathbf{C} = \mathbf{PK} \bmod 26$$

The Hill Algorithm

- C and P are row vectors of length 3 representing the plaintext and ciphertext,
- K is a 3 * 3 matrix representing the encryption key.
- Operations are performed mod 26.

$$(c_1\ c_2\ c_3) = (p_1\ p_2\ p_3)\begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix} \bmod 26$$

$$\mathbf{C} = \mathbf{PK} \bmod 26$$

The Hill Algorithm

Decryption Algorithm:

- $\mathbf{P} = D(\mathbf{K}, \mathbf{C}) = \mathbf{C}\mathbf{K}^{-1} \bmod 26$

The Hill Algorithm-Example

- Consider the plaintext “paymoremoney” and use the encryption key

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

- The first three letters of the plaintext “pay”= vector (15 0 24).
- Then(15 0 24)K = (303 303 531) mod 26 = (17 17 11) = RRL.

- Thus, the cipher text for the “paymoremoney”=RRLMWBKASPDH.

The Hill Algorithm

- Decryption requires using the inverse of the matrix **K**.

$$\mathbf{K}^{-1} = \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix}$$

$$\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} = \begin{pmatrix} 443 & 442 & 442 \\ 858 & 495 & 780 \\ 494 & 52 & 365 \end{pmatrix} \bmod 26 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

The Hill Algorithm

- The first three letters of the ciphertext “RRL”= vector (17 17 11).
- Then(17 17 11)K^{-1} mod 26= (15 0 24) = “pay”

- Thus, the plain text for the RRLMWBKASPDH= “paymoremoney”

The Hill Algorithm

- As with Playfair, the strength of the Hill cipher is that it completely hides single-letter frequencies.
- Indeed, with Hill, the use of a larger matrix hides more frequency information.
- A 3 * 3 Hill cipher hides not only single-letter but also two-letter frequency information
- Although the Hill cipher is strong against a ciphertext-only attack, it is easily broken with a known plaintext attack.

One-Time Pad

- An Army Signal Corp officer, Joseph Mauborgne, proposed an improvement to the Vernam cipher that yields the ultimate in security.

- Mauborgne suggested using a random key that is as long as the message, so that the key need not be repeated.

One-Time Pad

- In addition, the key is to be used to encrypt and decrypt a single message, and then is discarded.
- Each new message requires a new key of the same length as the new message.
- Such a scheme, known as a **one-time pad**, is unbreakable.

One-Time Pad

- Maintains perfect secrecy.
- Each plaintext symbol is encrypted with a key randomly chosen from a key domain
- Impossible to implement commercially as needs random keys be exchanged everytime

Strengths-One-Time Pad

- It produces random output that bears no statistical relationship to the plaintext.

- Because the ciphertext contains no information whatsoever about the plaintext, there is simply no way to break the code.

One-Time Pad-Example

- Suppose that we are using a Vigenère scheme with 27 characters in which the twenty-seventh character is the space character,
- A One-time key as long as the message.
- Consider the ciphertext

ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS

One-Time Pad-Example

- Two different decryptions using two different keys:

```
ciphertext: ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS
key:        pxlmvmsydofuyrvzwc tnlebnecvgdupahfzzlmnyih
plaintext:  mr mustard with the candlestick in the hall

ciphertext: ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS
key:        pftgpmiydgaxgoufhkllmhsqdqogtewbqfgyovuhwt
plaintext:  miss scarlet with the knife in the library
```

One-Time Pad-Example

- How is the cryptanalyst to decide which is the correct decryption?
- If the actual key were produced in a truly random fashion, then the cryptanalyst cannot say that one of these two keys is more likely than the other.
- Thus, there is no way to decide which key is correct and therefore which plaintext is correct.

Transposition Techniques

- Substitution-All the techniques involve the substitution of a ciphertext symbol for a plaintext symbol.

Transposition cipher-

- **A very different kind of mapping achieved by performing some sort of permutation on the plaintext letters.**

Transposition Techniques-Rail fence

- **The plaintext is written down as a sequence of diagonals and then read off as a sequence of rows.**
- For example, to encipher the message “meet me after the toga party” with a rail fence of depth 2, we write the following:

```
m e m a t r h t g p r y
  e t e f e t e o a a t
```

- The encrypted message is

MEMATRHTGPRYETEFETEOAAT

- Trivial to cryptanalyze

Transposition Techniques

A more complex scheme:

1) **Write the message in a rectangle, row by row**

2) **Read the message off, column by column**

3) **Permute the order of the columns**

4) **The order of the columns then becomes the key to the algorithm**

Transposition Techniques

For example,

```
Key:          4 3 1 2 5 6 7
Plaintext:    a t t a c k p
              o s t p o n e
              d u n t i l t
              w o a m x y z
Ciphertext:   TTNAAPTMTSUOAODWCOIXKNLYPETZ
```

Transposition Techniques

- **The key is 4312567.**
- **To encrypt, start with the column that is labeled 1, in this case column 3. Write down all the letters in that column.**
- **Proceed to column 4, which is labeled 2, then column 2, then column 1, then columns 5, 6, and 7.**

```
Key:          4 3 1 2 5 6 7
Plaintext:    a t t a c k p
              o s t p o n e
              d u n t i l t
              w o a m x y z
Ciphertext:   TTNAAPTMTSUOAODWCOIXKNLYPETZ
```

Transposition Techniques

- A pure transposition cipher is easily recognized because it has the same letter frequencies as the original plaintext.
- Cryptanalysis is fairly straightforward
- Involves laying out the ciphertext in a matrix and playing around with column positions.
- Digram and trigram frequency tables can be useful.

Transposition Techniques

- The transposition cipher can be made significantly more secure
- By performing more than one stage of transposition.
- The result is a more complex permutation that is not easily reconstructed.

Transposition Techniques

- If the foregoing message is re-encrypted using the same algorithm

```
Key:      4 3 1 2 5 6 7
Input:    t t n a a p t
          m t s u o a o
          d w c o i x k
          n l y p e t z
Output:   NSCYAUOPTTWLTMDNAOIEPAXTTOKZ
```

Transposition Techniques

- As an example, let's encrypt the message "The tomato is a plant in the nightshade family" using the keyword *tomato*. We get the grid given below.

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

Transposition Techniques

- As an example, we shall decrypt the ciphertext "ARESA SXOST HEYLO IIAIE XPENG DLLTA HTFAX TENHM WX" given the keyword *potato*.
- We start by writing out the keyword and the order of the letters.
- There are 42 letters in the ciphertext, and the keyword has six letters, so we need 42 ÷ 6 = 7 rows.

P	O	T	A	T	O
4	2	5	1	6	3

Transposition Techniques

- Now we start by filling in the columns in the order given by the alphabetical order of the keyword, starting with the column headed by "A". After the first column is entered we have the grid shown to the right.

P	O	T	A	T	O
4	2	5	1	6	3
			A		
			R		
			E		
			S		
			A		
			S		
			X		

Transposition Techniques

- We continue to add columns in the order specified by the keyword.

P	O	T	A	T	O
4	2	5	1	6	3
			A		
			R		
			E		
			S		
			A		
			S		
			X		

P	O	T	A	T	O
4	2	5	1	6	3
	O		A		
	S		R		
	T		E		
	H		S		
	E		A		
	Y		S		
	L		X		

P	O	T	A	T	O
4	2	5	1	6	3
	O		A		O
	S		R		I
	T		E		I
	H		S		A
	E		A		I
	Y		S		E
	L		X		X

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

- Now we read off the plaintext row at a time to get "potatoes are in the nightshade family as well".

https://crypto.interactive-maths.com/columnar-transposition-cipher.html#decrypt

Combining Two Approaches

Example

Figure