Distributed and Edge Computing

Distributed Systems Security

Sharad K. Ghimire

Department of Electronics and Computer Engineering
Pulchowk Campus
Institute of Engineering
Tribhuvan University

Distributed Systems Security

Introduction

Overview of cryptography and data privacy

Security issues and techniques in distributed system

Security challenges in edge computing

Introduction to digital forensics

Contents

Security

The word 'secure' Derived from Latin securus, meaning freedom from anxiety: se (without) + cura (care, anxiety)

Security ?

The state of being free from danger or threat

Security can be defined as being free from danger, or feeling safe

Protection of a person, building, organization, or country against threats such as crime or attacks by foreign countries or terrorist

Security (Related with IT)

Security is all about protecting valuables

Here the “valuables” are computer related assets instead of money

In these days the protection of money is a subset of computer asset security

Information seems to be the currency of the 21st century

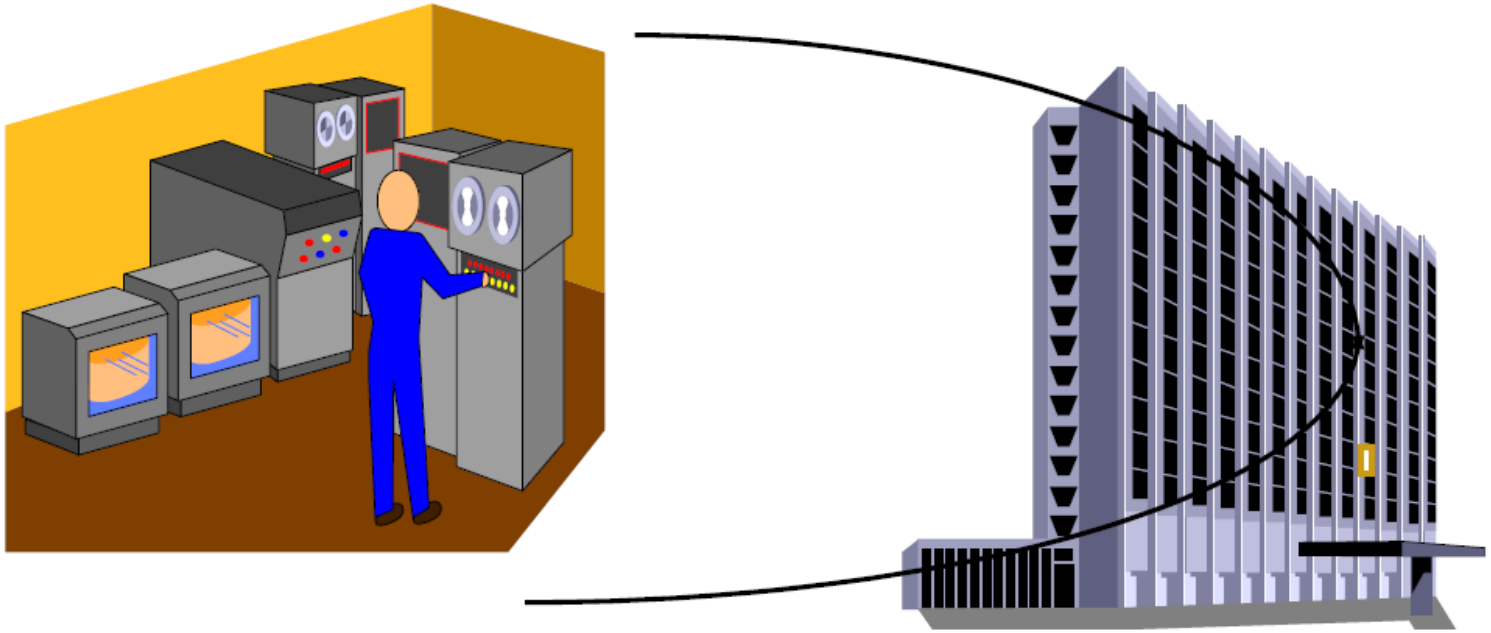
The protection of computer systems and networks from the theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide

Why Security

Past: Computers and computer communication were primarily used by university researchers for sending email and by corporate employees for sharing resources ⇒ security was not the issue

Now: The millions of ordinary citizens are using network communications for banking, shopping, using e-payment systems and many more, so weakness after weakness has been found ⇒ security become a great issue

Past Situation (Single System)



Physical security and control of access to computers

Current Situation

Why Security

When credit card payments over the Internet were first considered ⇒ traffic between customer and merchant need to be protected

Danger might be scanning Internet traffic for packets containing credit card numbers is an attack with a low yield

SSL was developed to deal with this problem

Badly protected servers at a merchant site holding a database of customer credit card numbers are a much more rewarding target and such attacks have occurred, either to obtain credit card numbers or to blackmail the merchant

Identity theft

Security Engineering

A field of engineering that focuses on the security aspects during design of systems that need to be able to deal robustly with possible sources of disruption, ranging from natural disasters to malicious acts

Security engineering is about **building systems to remain dependable in the face of malice, error, or mischance**

We can say that security engineering has **a goal to raise the effort for an attack to a level where the costs exceed the attacker's gains**

Security Requirements

Security Requirements

Confidentiality –

- Protect data contents and access

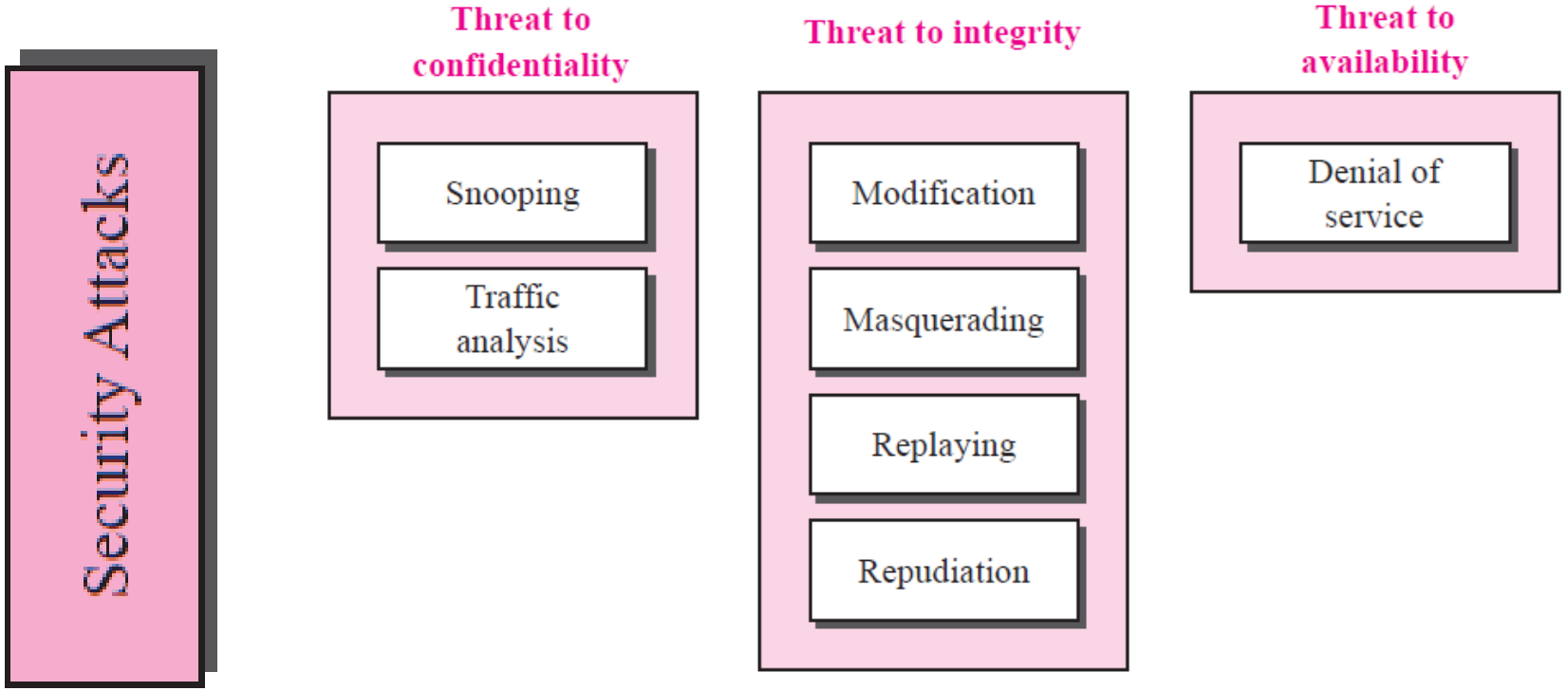
Integrity –

- Protect data accuracy

Availability –

- Ensure timely service

Threats


Security Attacks
Threat to confidentiality
Snooping
Traffic analysis
Threat to integrity
Modification
Masquerading
Replaying
Repudiation
Threat to availability
Denial of service

Threats to confidentiality

Snooping:

- Unauthorized access to or interception of data

Traffic Analysis:

- Encipherment of data may make it non-intelligible for the interceptor, but s/he can obtain some other type information by monitoring online traffic, e.g. find the electronic address of sender and receiver and guess the nature of transaction and so on

Threats to integrity

Modification: Modification of information to make it beneficial

Masquerading: Masquerading or spoofing, happens when the attacker impersonates somebody else. For example, an attacker might steal the bank card and PIN of a customer and pretend that s/he is that customer

Replaying: Attacker obtains a copy of a message sent by a user and later tries to replay it

Repudiation: This type of attack is different from others because it is performed by one of the two parties in the communication; either the sender or the receiver. The sender of the message might later deny that she has sent the message

Threats to availability

Denial of Service:

A very common attack

It may slow down or totally interrupt the service of a system by using various techniques

Attacks Types

Classifying security attacks (RFC 2828) in terms of passive and active attacks:

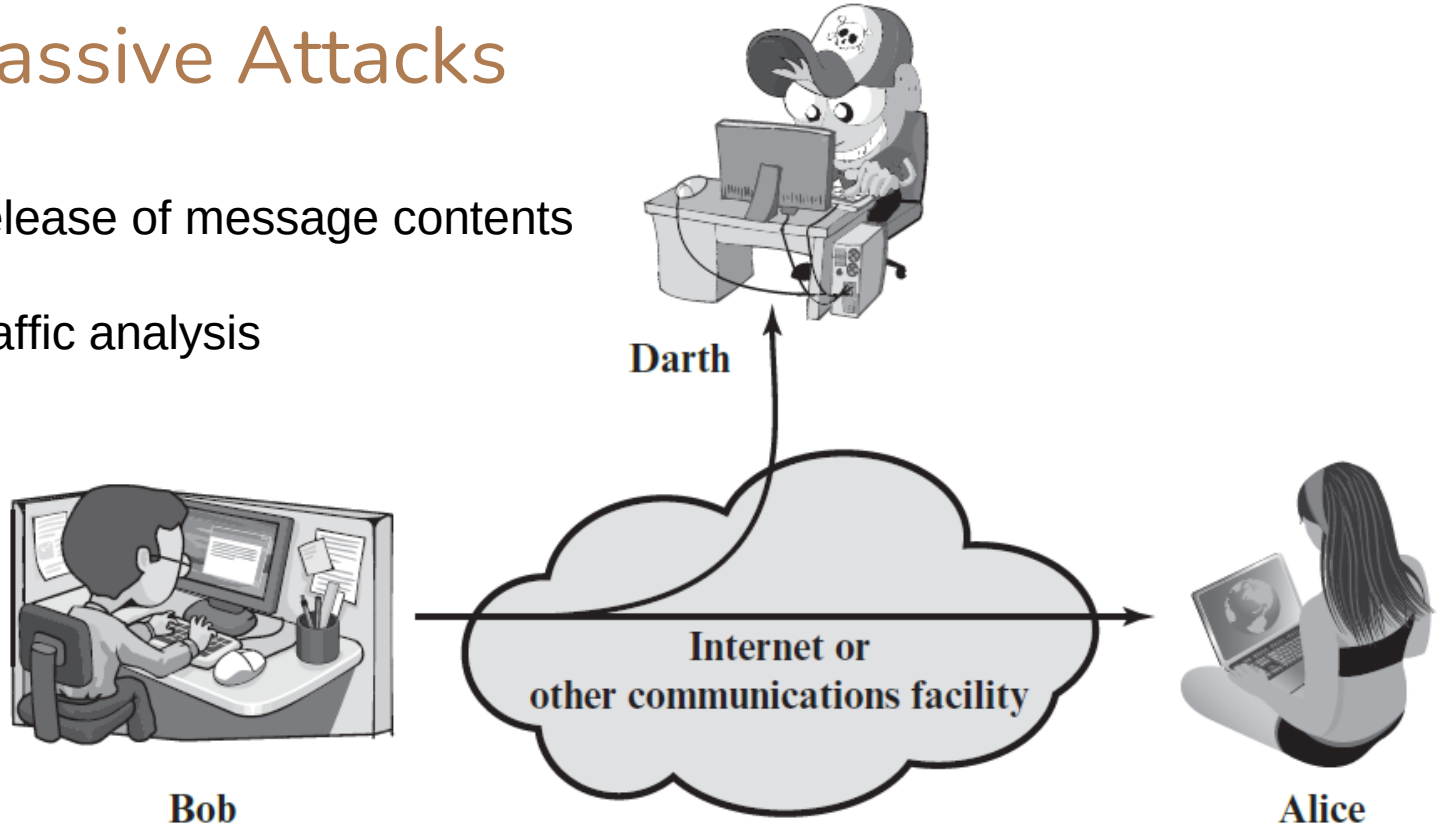
Passive attack: Attempts to learn or make use of information from the system but does not affect system resources

Active attack: Attempts to alter system resources or affect their operation

Passive Attacks

Release of message contents

Traffic analysis



Passive Attacks

Attempt to learn or make use of information from the system but do not affect system resources

To obtain information

- Release of possibly sensitive/confidential message contents
- Traffic analysis which monitors frequency and length of messages to get info on senders

Difficult to detect

But relatively easy to prevent, can be prevented using encryption

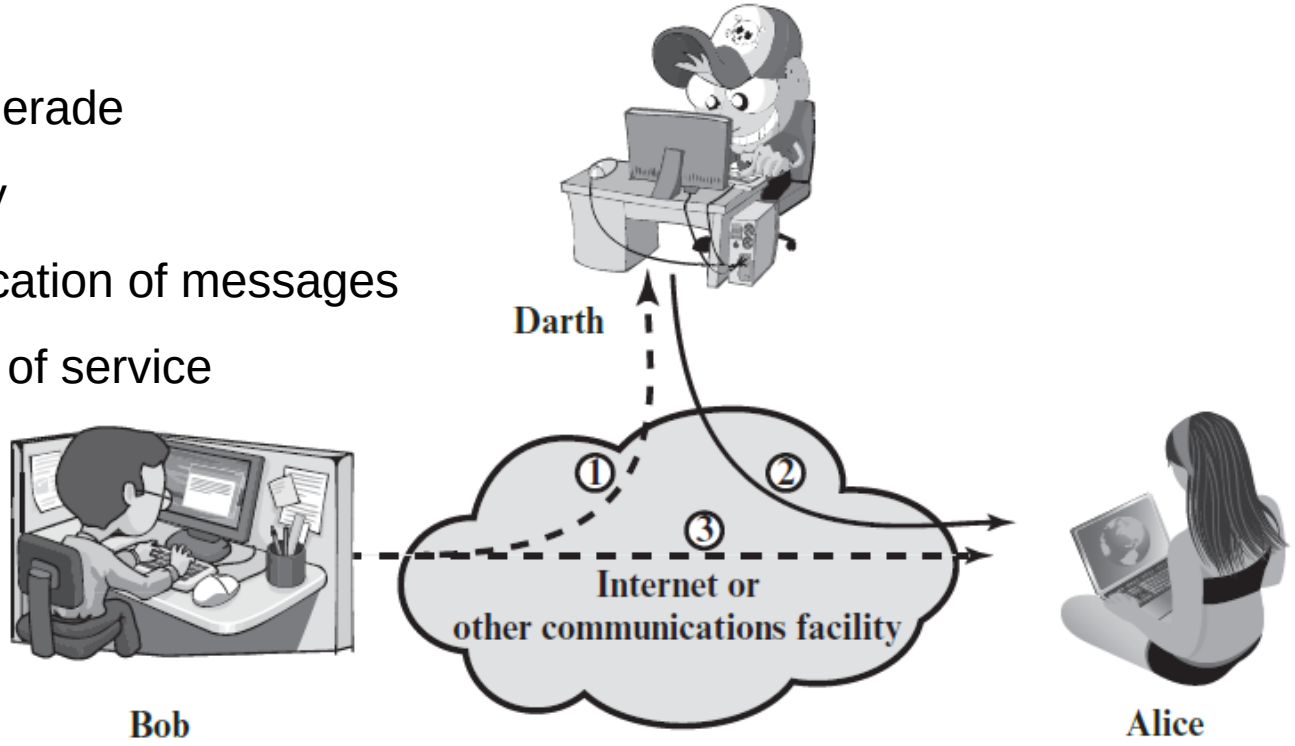
Active Attacks

Masquerade

Replay

Modification of messages

Denial of service



Active Attacks

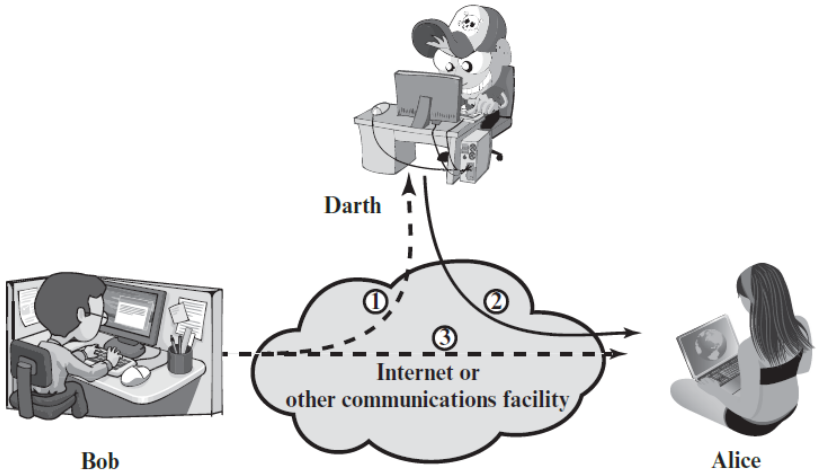
Active attack attempts to alter system resources or affect their operation

- Masquerade
- Replay
- Modification of messages
- Denial of service

Easy to detect

Hard to prevent

Focus on detection and recovery



Techniques

Some techniques are used for implementation of security goals:

Cryptography

- Greek origin meaning - “secret writing”
- Transforming message to make them secure and immune to attacks

Steganography

- Greek origin meaning - “covered writing”
- Concealing the message itself by covering it with something else

Cryptography

Cryptography, a word with Greek origins means “secrete writing”

From Ancient Greek: translit "hidden, secret"; and graphein, "**to write**", or "**study**" - **practice and study** of techniques for secure communication

Cryptography

An art of achieving security by encoding messages to make them non-readable i.e. to introduce secrecy

Process of hiding or coding information so that only the intended person or system can read it

Has been used to encode messages for thousands of years

Historically, four groups of people have used and contributed to the art of cryptography: Military, Diplomatic groups, Diarists, and Lovers

Cryptography (contd...)

It is being used in credit cards, computer passwords, ecommerce and many more in nowadays

It is about constructing and analyzing protocols that prevent third parties or the public from reading the private messages

Importance is being increased day by day

Cryptography (contd...)

In the early days, cryptography used to be performed by using manual techniques

For example, let the message were the word "private" can be converted in to different form to yield TVMZEXI so that it cannot be easily understood by anyone

Initially it seems to be difficult to crack but once the algorithm is known, the secrecy is lost

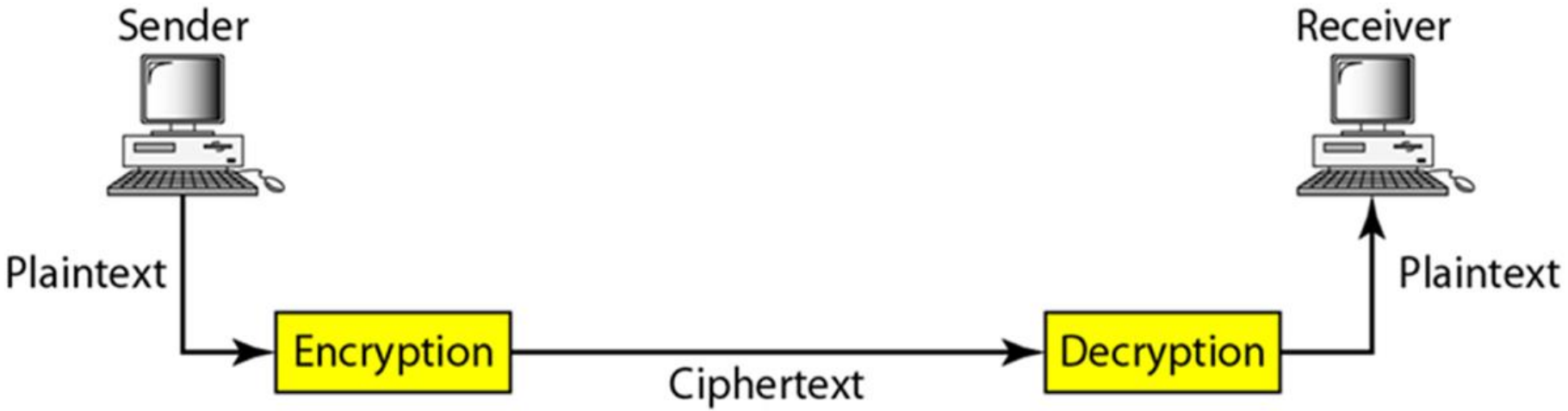
Cryptography (contd...)

Some cryptographic algorithms are very trivial to understand, replicate and therefore easy to crack

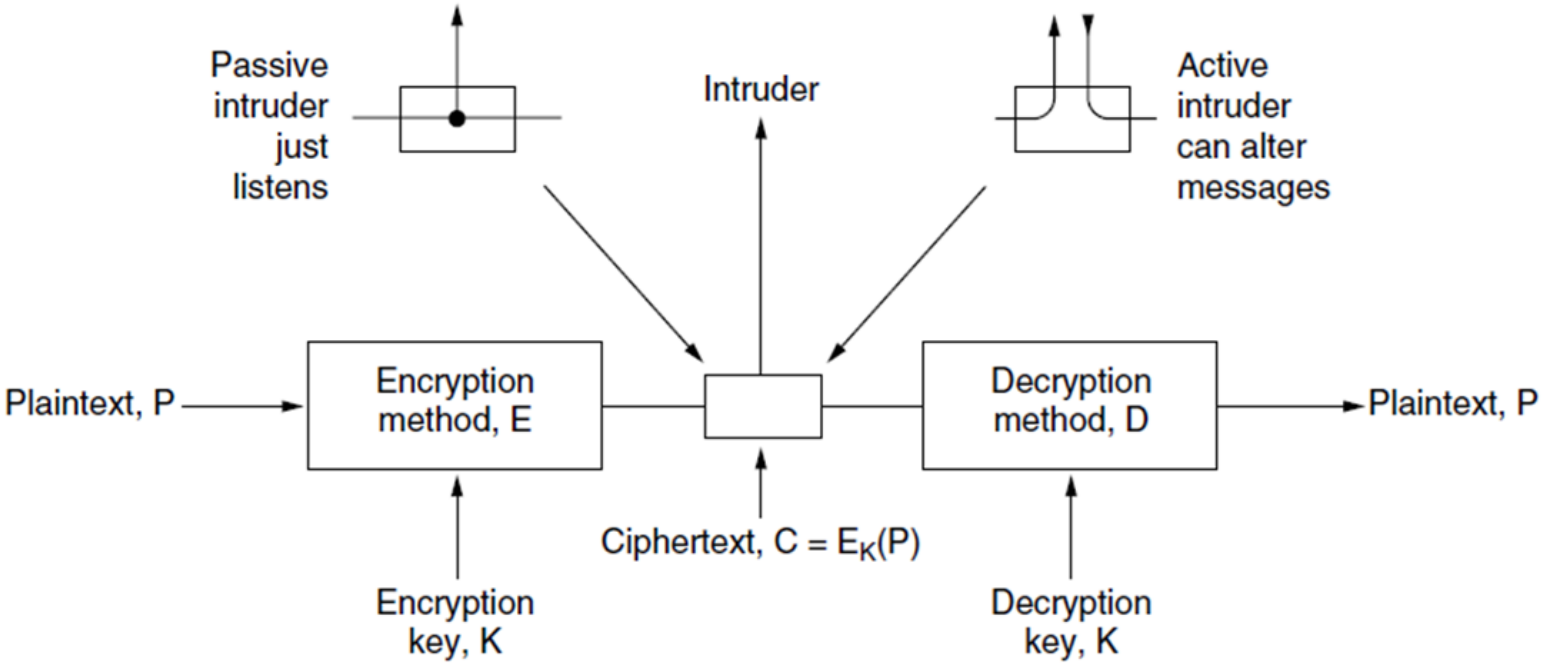
Some other cryptography algorithms are highly complicated and therefore difficult to crack

The rest are somewhere in the middle

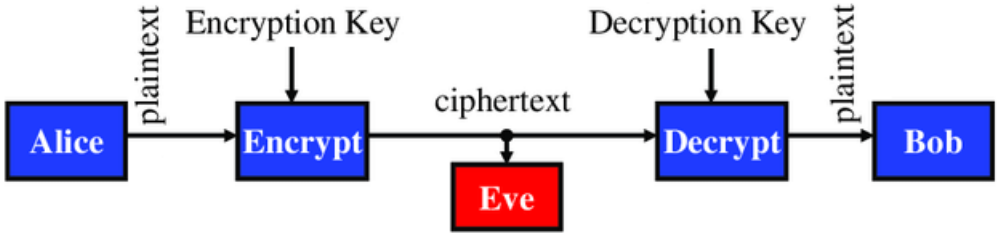
Cryptography Components



Encryption Model



Terminologies



Plaintext:- Refers to a message in plain form, i.e. the original message that is readily intelligible (also called cleartext)

Encryption:- Process of disguising the message to hide it from unwanted ones

Ciphertext:- A disguised message obtained by encryption process to the plaintext

Decryption:- The process of extracting the plaintext from ciphertext

Cipher:- An algorithm used for performing encryption or decryption

Key:- A value (or stream of characters or bits) that is applied in cryptography to get ciphertext from plaintext or plaintext from ciphertext

History of Cryptography


Hieroglyph

Caesar Cipher

Around 100 BC, Julius Caesar was known to use a form of encryption to convey secret messages to his army generals posted in the war front

This substitution cipher, known as **Caesar cipher**, is perhaps the most mentioned historic cipher in academic literature

In a substitution cipher, each character of the plain text is substituted by another character to form the cipher text

It was a shift by 3 cipher, i.e., each character was shifted by 3 places, so the character 'A' was replaced by 'D', 'B' by 'E', and so on

History of Cryptography (contd...)

Up to the Second World War, most of the work on cryptography was for military purposes, usually used to hide secret military information

Cryptography attracted commercial attention post-war, with businesses trying to secure their data from competitors

In the early 1970's, IBM realized that their customers were demanding some form of encryption, so they formed a "crypto group" headed by Horst-Feistel ⇒ designed a cipher called **Lucifer**

History of Cryptography (contd...)

In 1973, the Nation Bureau of Standards (now called NIST) in the US put out a request for proposals for a block cipher which would become a national standard ⇒ Lucifer was eventually accepted and was called **DES** or the **Data Encryption Standard**

In 1997, and in the following years, DES was broken by an exhaustive search attack (using high processing power of computer)

The main problem with DES was the small size of the encryption key

History of Cryptography (contd...)

As computing power increased it became easy to brute force all different combinations of the key to obtain a possible plain text

In 1997, NIST again put out a request for proposal for a new block cipher ⇒ which received several submissions

In 2000, it accepted Rijndael, and christened it as **AES** or the **Advanced Encryption Standard**

Now AES is a widely accepted standard used for symmetric encryption

Kerckhoffs's Principle

Stated by Dutch-born cryptographer Auguste Kerckhoffs in the 19th century, also known as Kerckhoff's law ⇒ a principle in cryptography

According to the principle, a cryptosystem should be secure, even if everything about the system, except the key, is public knowledge

Referred to as "security through obscurity is not the security", i.e. opposite to the idea of "security through obscurity"

This concept is widely embraced by many cryptographers

Kerckhoffs's Principle (contd...)

Based on the idea that the security of a cryptographic system should not depend on the secrecy of its algorithm, design or implementation

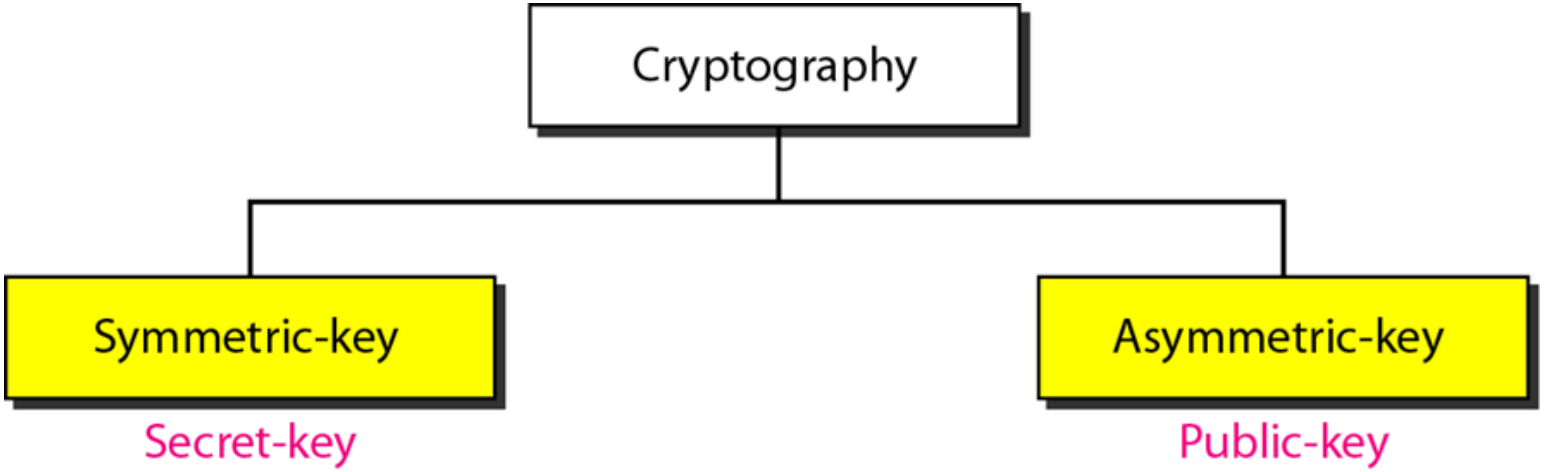
Instead, the security of the system should depend solely on the secrecy of the key that should be kept secrete

A security system is secure only if its details can be shared with the world

Allows others to verify the security of the protocol without compromising the security of the system

Cryptography Categories

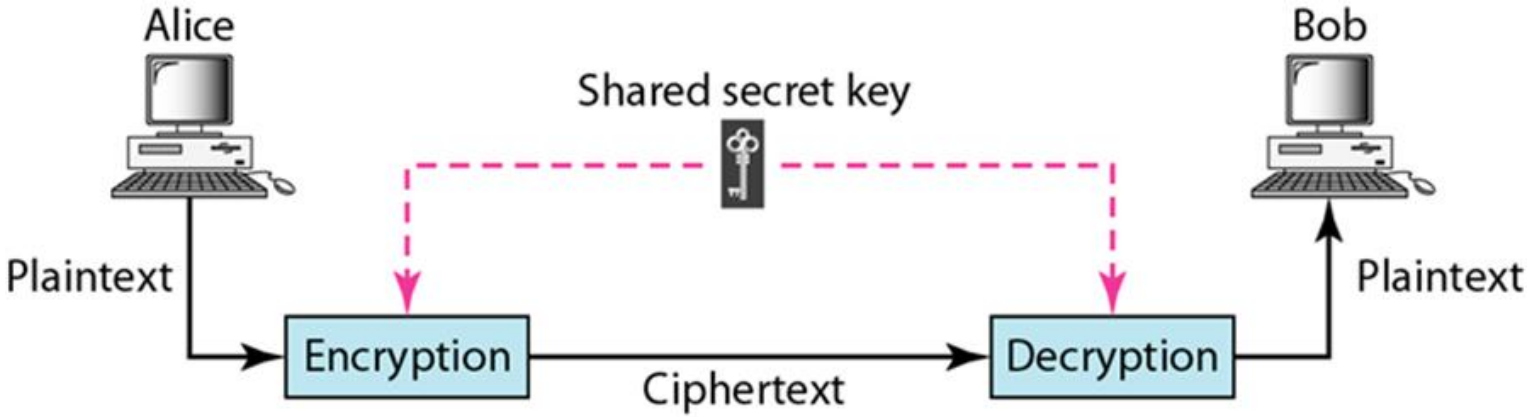
Categories of Cryptography



Symmetric-key Cryptography

Same key is used by the sender (for encryption) and the receiver (for decryption)

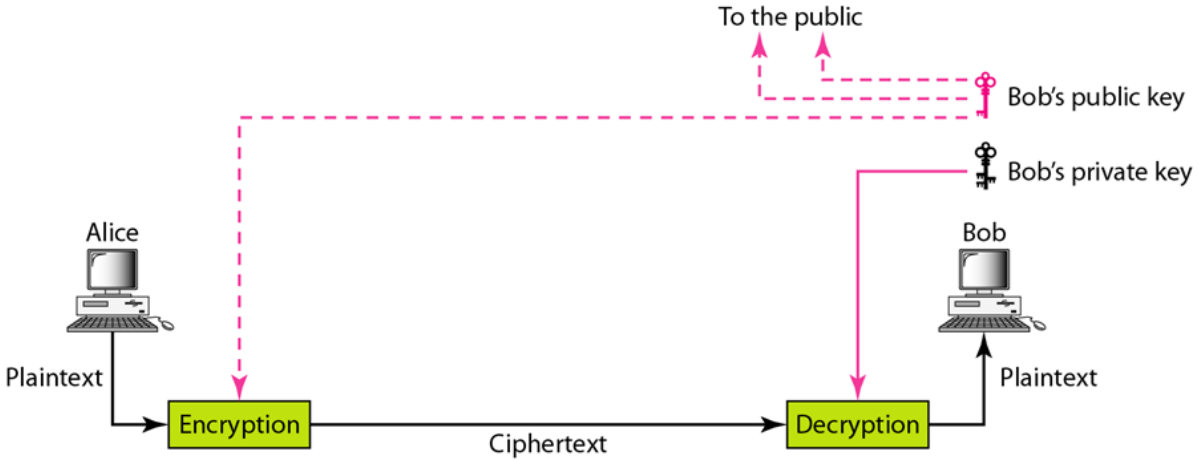
The key need to be shared between sender and receiver

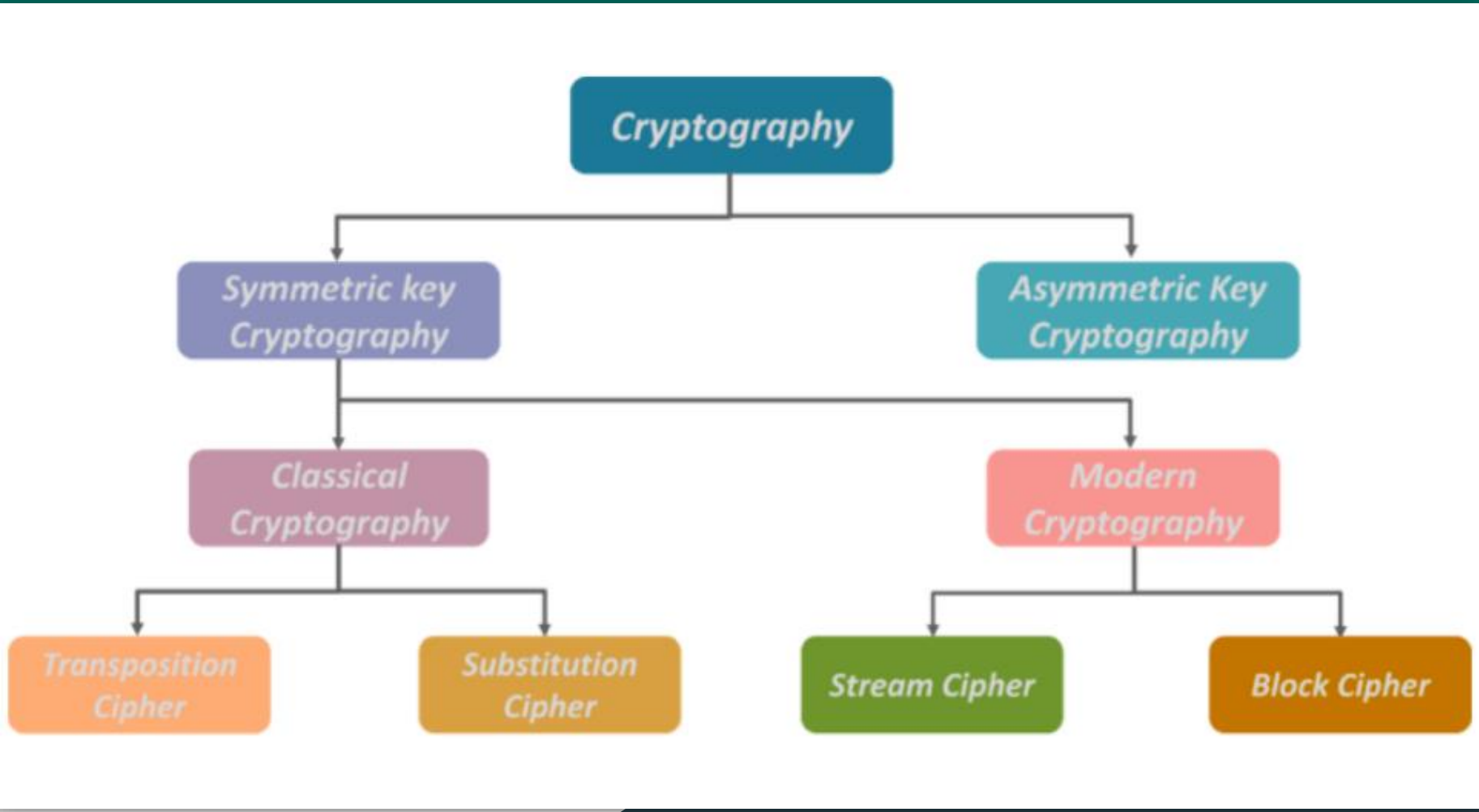


Asymmetric-key Cryptography

There are two keys: A private key and a public key

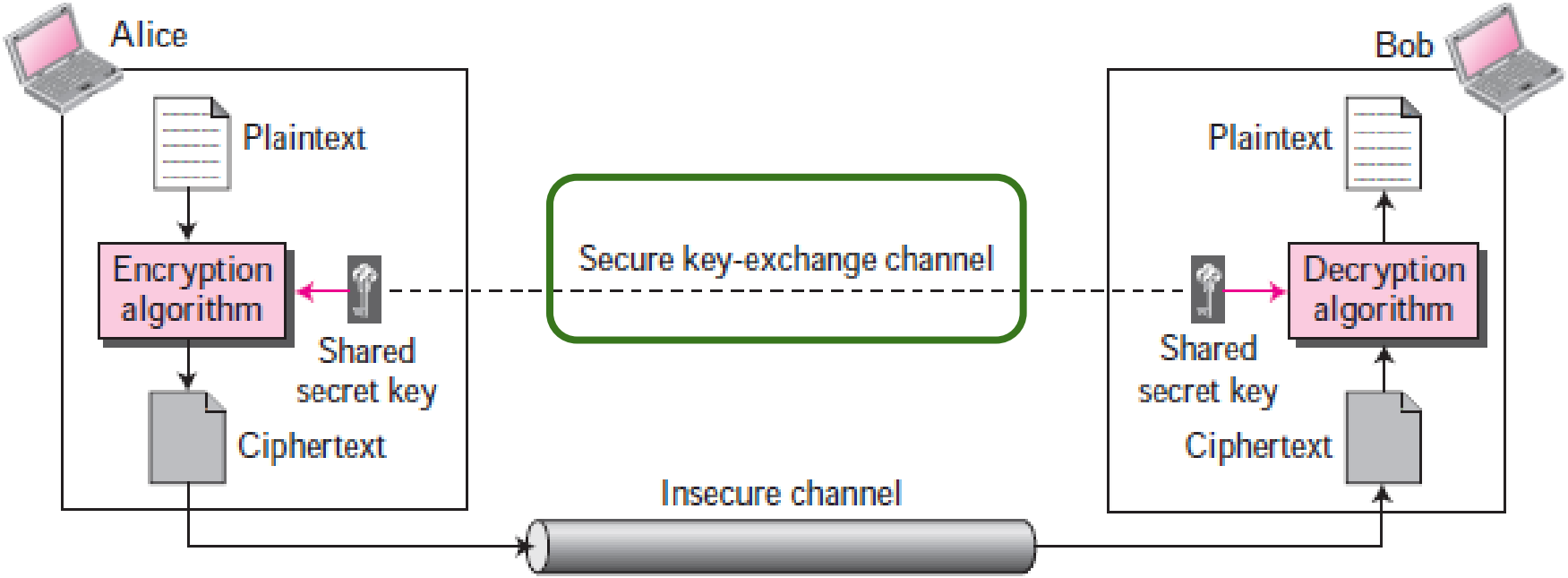
Private key is kept by receiver and Public key is announced to the public




Cryptography
Symmetric key Cryptography
Asymmetric Key Cryptography
Classical Cryptography
Modern Cryptography
Transposition Cipher
Substitution Cipher
Stream Cipher
Block Cipher

Symmetric Encryption

Symmetric Encryption



Symmetric Encryption (contd...)

Symmetric encryption, also referred to as conventional encryption or single-key encryption, was the only type of encryption in use prior to the development of public key encryption in the 1970s

It remains by far the most widely used from very early days (thousand years ago) to present days as well

Symmetric Encryption (contd...)

Universal technique for providing confidentiality for the transmitted data

Also referred to as conventional encryption or single-key encryption

Was the only type of encryption in use prior to the introduction of public-key encryption

In many cases, from Julius Caesar to diplomatic, military, and several commercial users, have used symmetric encryption for secret communication

Symmetric Encryption (contd...)

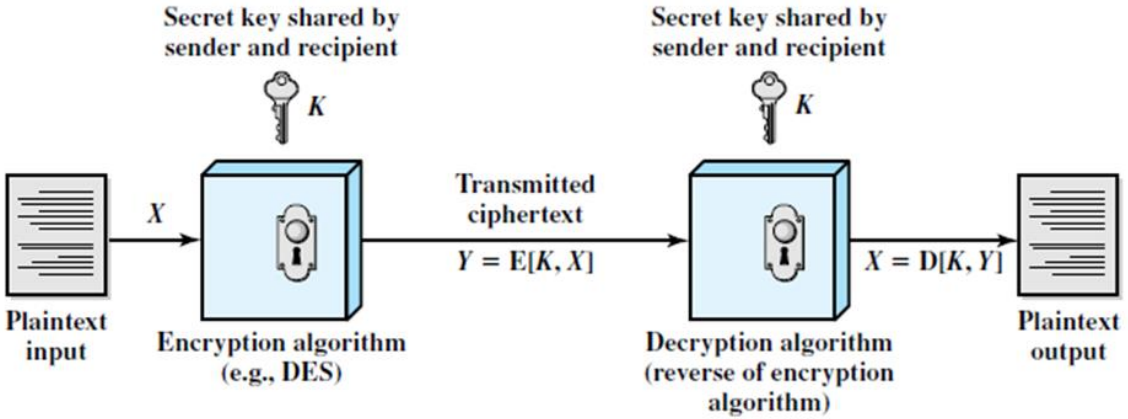
Plaintext

Encryption Algorithm

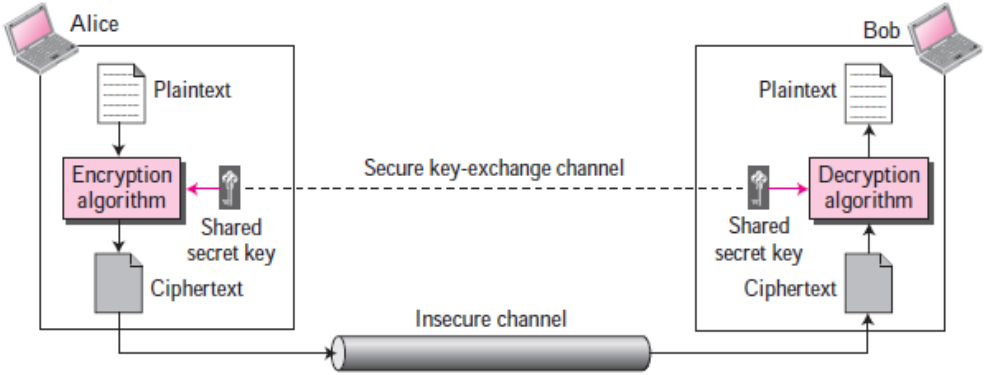
Secret Key

Ciphertext

Decryption Algorithm



Symmetric Encryption (contd...)



If P is the plaintext, C is the ciphertext, and K is the key, then

- Encryption algorithm Ek(x) creates the ciphertext from the plaintext
- Decryption algorithm Dk(x) creates the plaintext from the ciphertext

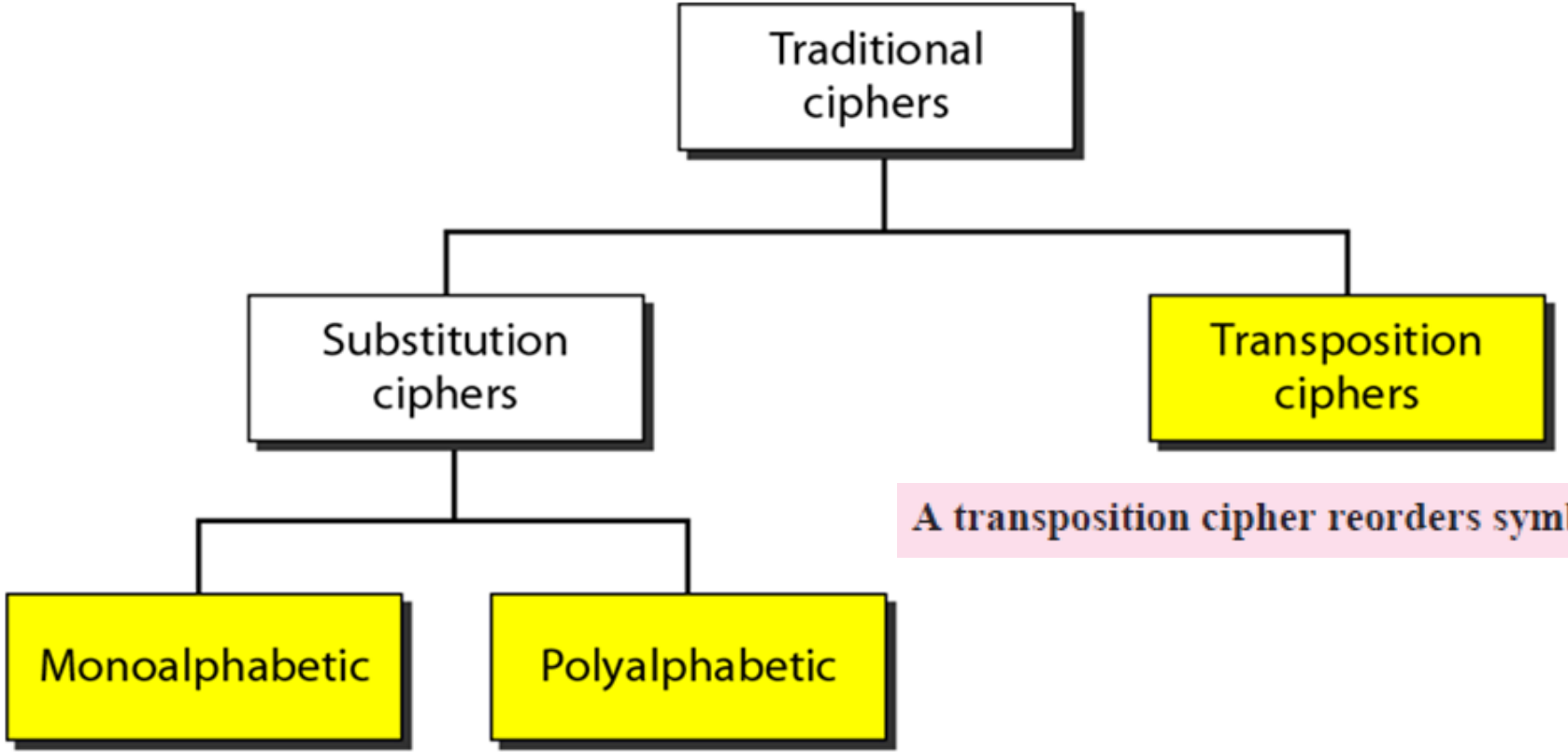
Ek(x) and Dk(x) are inverses of each other: they cancel the effect of each other if they are applied one after the other on the same input

Since, we have

- Encryption: C = Ek(P)
- Decryption: P = Dk(C)

⇨ Dk(Ek(x)) = Ek(Dk(x)) = x

Classical Cryptography (Traditional Ciphers)



A transposition cipher reorders symbols.

A substitution cipher replaces one symbol with another.

Substitution Ciphers

Any character of plain text from the given fixed set of characters is substituted by some other character from the same set depending on a key

For example with a shift of 1, A would be replaced by B, B would become C, and so on

The simple substitution cipher is a cipher that has been in use for many hundreds of years

The simple substitution cipher offers very little communication security

Substitution Cipher (contd...)

Plaintext: HELLO
Ciphertext: KHOOR

In a substitution cipher, each character of the plain text is substituted by another character to form the cipher text

Let a plaintext “hello” and its corresponding ciphertext using monoalphabetic cipher as “KHOOR”

Similarly, let us see the same plaintext and its corresponding ciphertext using polyalphabetic cipher as “ABNZF”

Plaintext: HELLO
Ciphertext: ABNZF

Monoalphabetic Cipher

A character (or a symbol) in the plaintext is always changed to the same character (or symbol) in the ciphertext regardless of its position in the text, e.g. if a letter A in the plaintext is changed to letter D, every letter A is changed to letter D

The relationship between letters in the plaintext and the ciphertext is one-to-one

The simplest monoalphabetic cipher is the additive cipher (or shift cipher)

Shift cipher

One of the simplest cipher

For convenient mathematical operations numerical values can be used for each letter

The plaintext, ciphertext, and key are integers in modulo 26

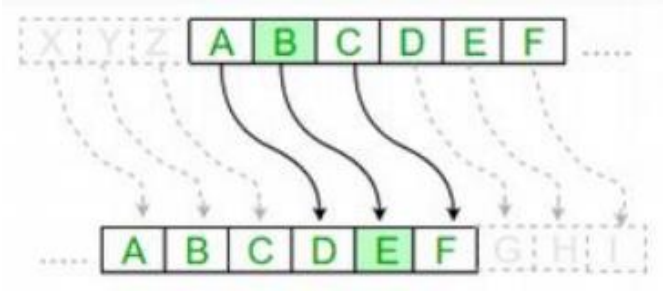
Julius Caesar used an additive cipher, with a key of 3 to communicate with his officers ⇨ additive ciphers are sometimes referred to as the **Caesar** cipher

Caesar Cipher

Plain Text : 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 Text : 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

$$C_i = E(P_i) = P_i + 3$$



The message “**hello**” is enciphered as ⇨ “**KHOOR**”

Example - Encryption

Use the additive cipher with key = 15 to encrypt the message “hello”

Solution

Plaintext: h → 07	Encryption: (07 + 15) mod 26	Ciphertext: 22 → W
Plaintext: e → 04	Encryption: (04 + 15) mod 26	Ciphertext: 19 → T
Plaintext: l → 11	Encryption: (11 + 15) mod 26	Ciphertext: 00 → A
Plaintext: l → 11	Encryption: (11 + 15) mod 26	Ciphertext: 00 → A
Plaintext: o → 14	Encryption: (14 + 15) mod 26	Ciphertext: 03 → D

The result is “WTAAD”

Example - Decryption

Use the additive cipher with key = 15 to decrypt the message “WTAAD”

Solution

Ciphertext: W → 22 Decryption: (22 − 15) mod 26 Plaintext: 07 → h

Ciphertext: T → 19 Decryption: (19 − 15) mod 26 Plaintext: 04 → e

Ciphertext: A → 00 Decryption: (00 − 15) mod 26 Plaintext: 11 → l

Ciphertext: A → 00 Decryption: (00 − 15) mod 26 Plaintext: 11 → l

Ciphertext: D → 03 Decryption: (03 − 15) mod 26 Plaintext: 14 → o

The result is “hello”

Caesar Cipher

These kinds of ciphers depend on the secrecy of the system and not on the encryption key

Once the system is known, the encrypted messages can easily be decrypted

Very limited no of possible keys

Monoalphabetic substitution ciphers

Example:

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

Let us see the plain text:

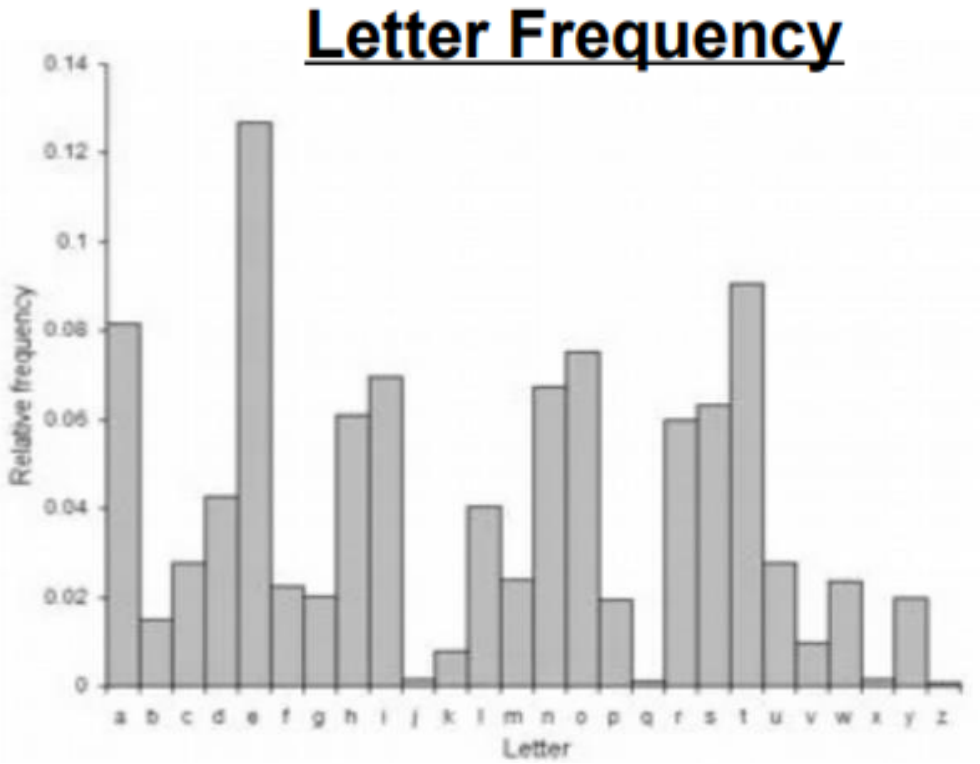
this message is easy to encrypt but not easy to find the key

Then the ciphertext becomes:

ICFVQRVVNEFVRNVSIYRGAHSLIOJICNHTIYBFGTICRXRS

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



Monoalphabetic Substitution

Polyalphabetic Ciphers

Each occurrence of a single character may have a different substitute

One-to-many relationship between a character in the plaintext to a character in the ciphertext

Can hide the letter frequency of the underlying language

Intruder like Eve cannot use single-letter frequency statistics to break

Ciphertext character is dependent on both the corresponding plaintext character and the position of the plaintext character in the message

Polyalphabetic Substitutions Example

Table for Odd Positions

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

Table for Even Positions

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

Plain Text: **ssibl**

Cipher Text: **CZYSH**

Vigenere cipher

Invented by the French cryptographer Blaise de Vigenère in the 16th century to encrypt and decrypt messages

Easy to understand and implement and has a long history of usage

Uses simple form of polyalphabetic substitution cipher ⇒ uses multiple cipher alphabets to encrypt the plaintext

For many years it was considered as literally “the unbreakable cipher”

Gained a reputation for being very strong because resisted all attempts to break around up to **three centuries**

Vigenere cipher

A sequence of text is used as a key

The encryption key was repeated multiple times spanning the entire message, and then the cipher text was produced by adding the message character with the key character modulo 26

Encryption

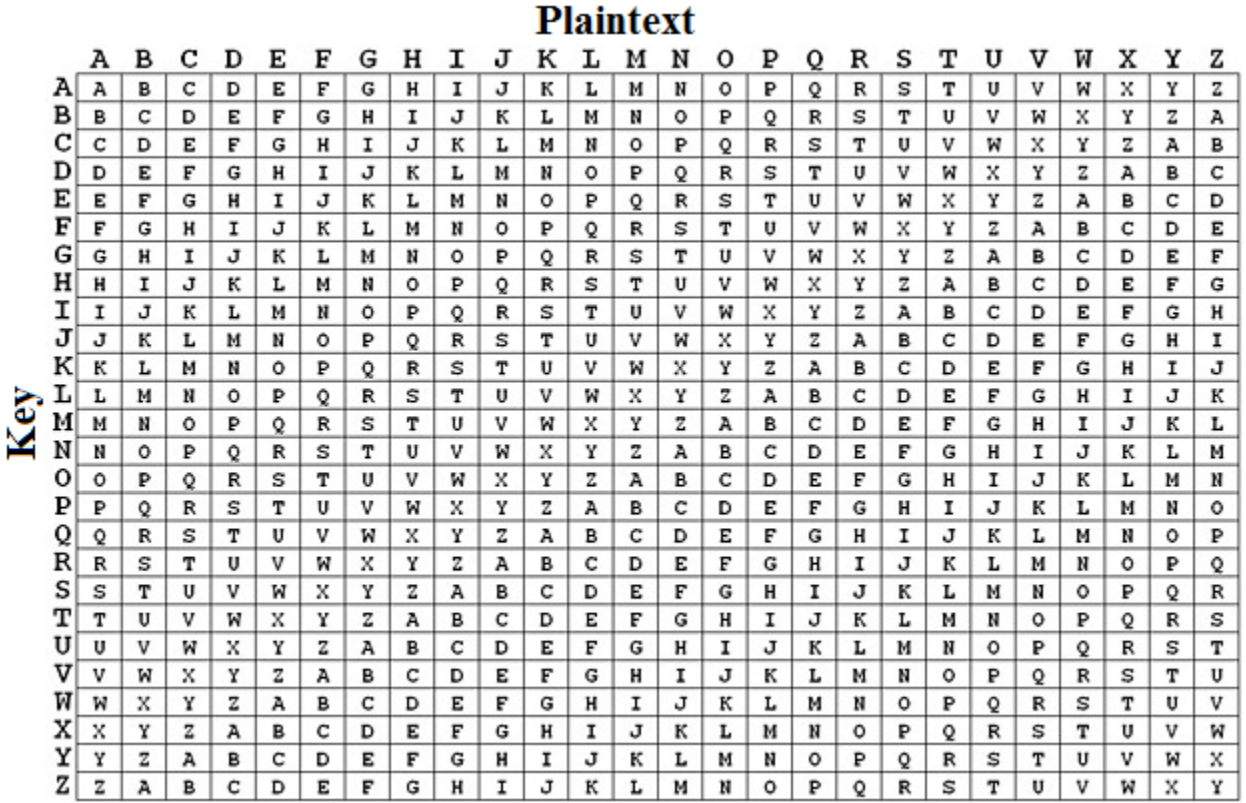
The plaintext(P) and key(K) are added modulo 26

Ei = (Pi + Ki) mod 26

Decryption

Di = (Ei - Ki) mod 26

computer → Encryption → EFKESHGI



Vigenere Cipher Table

Example

Encryption

plaintext	m	a	t	h	i	s	f	u	n
m_i	12	0	19	7	8	18	5	20	13
keyword	j	i	m	j	i	m	j	i	m
k_i	9	8	12	9	8	12	9	8	12
$c_i \equiv m_i + k_i \pmod{26}$	21	8	5	16	16	4	14	2	25
ciphertext	v	i	f	q	q	e	o	c	z

Ciphertext: vifqqeocz

Example

Decryption

ciphertext	v	i	f	q	q	e	o	c	z
c_i	21	8	5	16	16	4	14	2	25
d_i	17	18	14	17	18	14	17	18	14
$m_i \equiv c_i + d_i \pmod{26}$	12	0	19	7	8	18	5	20	13
plaintext	m	a	t	h	i	s	f	u	n

Plaintext: math is fun

Vigenere cipher

The first cipher brought the idea of introducing encryption keys

Comparing this to Caesar cipher, the secrecy of the message depends on the secrecy of the encryption key, rather than the secrecy of the system ⇒ Kerckhoff's principle

Not so secure

Transposition Ciphers

Transposition Cipher

Also known as a permutation cipher

A method that scrambles the positions of characters (transposition) without changing the characters themselves

Reorder units of plaintext (typically characters or groups of characters) according to a regular system to produce a ciphertext which is a permutation of the plaintext

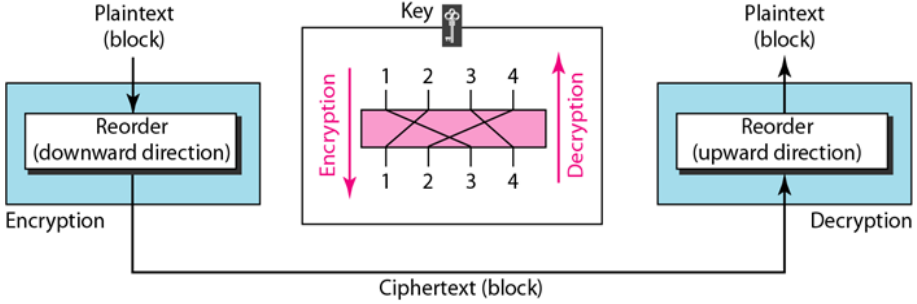
Differ from substitution ciphers, which do not change the position of units of plaintext but instead change the units themselves

Transposition Cipher

The substitution ciphers are based on the replacing plaintext symbol with a ciphertext symbol

Here the mapping is achieved by performing some sort of permutation on the plaintext letters ⇒ referred to as a transposition cipher

Transposition Cipher

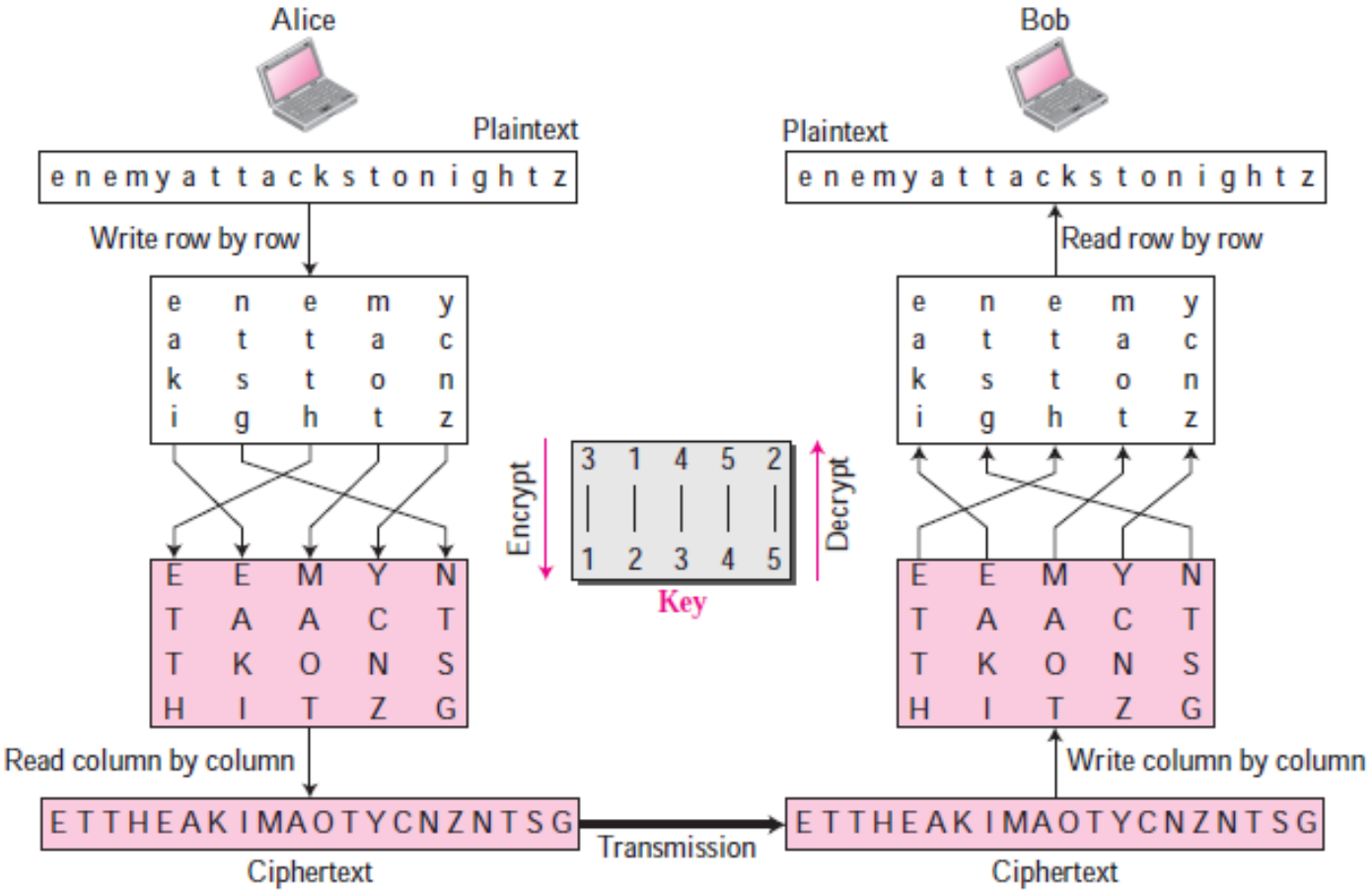


There is no substitution of characters instead their locations changed

It reorders (permutes) symbols in a block of symbols

Key is the mapping between the position of the symbols in plaintext and ciphertext

Transposition Cipher Example



Transposition Cipher

A pure transposition cipher is easily recognized because it has the same letter frequencies as the original plaintext

For the type of columnar transposition just shown, cryptanalysis is fairly straightforward and involves laying out the ciphertext in a matrix and playing around with column positions

The transposition cipher can be made significantly more secure by performing more than one stage of transposition

The result become more complex permutation that is not easily reconstructed

Cryptography Attacks

Cryptography Attacks

Malicious attempts to compromise the security of cryptographic systems

Aims to exploit vulnerabilities and gain unauthorised access to sensitive information

Attacks cause threats to the confidentiality, integrity, and availability of encrypted data

Attackers employ various strategies to breach cryptographic defences, targeting weaknesses in algorithms, keys, or implementation processes

Types of cryptanalytic attacks

Cipher text only – A copy of cipher text alone is known to the cryptanalyst

Known plaintext – The cryptanalyst has a copy of the cipher text and the corresponding plaintext

Chosen plaintext – The cryptanalysts can encrypt a large number of suitably chosen plaintexts and try to use the resulting cipher texts to deduce the key

Chosen cipher text – The cryptanalyst decrypt several string of symbols, and tries to use the results to deduce the key

Brute Force

Using a systematic method of trying every possible key until the correct one is found

Involves an exhaustive trial-and-error approach, making it time-consuming but effective if encryption keys are weak or easily guessable

Can target various cryptographic systems, including passwords, encryption keys, and digital signatures

To mitigate the risk of brute force attacks, use of strong and complex encryption keys is essential

Brute Force

Longer and complex keys exponentially increase the time and computational resources for attackers to succeed

The effectiveness of cryptographic defences relies on the resilience against brute force attempts, emphasising the importance of robust key management practices in the digital security landscape

Preventing Cryptography Attacks

Cryptographic attacks pose a substantial threat to the security of sensitive information, necessitating robust preventive measures to safeguard against potential breaches

Implementing effective strategies involves a multifaceted approach

Preventing Cryptography Attacks

Use strong encryption technique and unique keys for encryption

Regularly update the cryptographic algorithms and protocols to ensure they are not obsolete

Secure the keys

Ensure that the cryptographic system is implemented correctly

Regularly test the system for vulnerabilities

Requirements for Security

Strong encryption algorithm

- Even algorithm is known, unable to decrypt without key
- Even if plaintexts & ciphertexts available, unable to find the key

Sender and receiver must **share secret key securely**

Once key is known, all communication using this key is readable

Now it can be broken within few minutes due to the processing power of current computers

Key Size (bits)	Number of Alternative Keys	Time Required at 1 Decryption/μs	Time Required at 10^6 Decryptions/μs
32	$2^{32} = 4.3 \times 10^9$	$2^{31}\ \mu s = 35.8$ minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	$2^{55}\ \mu s = 1142$ years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	$2^{127}\ \mu s = 5.4 \times 10^{24}$ years	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	$2^{167}\ \mu s = 5.9 \times 10^{36}$ years	5.9×10^{30} years
26 characters (permutation)	$26! = 4 \times 10^{26}$	$2 \times 10^{26}\ \mu s = 6.4 \times 10^{12}$ years	6.4×10^{6} years

Table: Average Time Required for Exhaustive Key Search

Goals of Cryptography

Services provided by cryptography

- Confidentiality (secrecy)
- Integrity (anti-tampering)
- Authentication
- Non-repudiation