Cryptography

Classification of Cryptography
Cryptoanalysis
Symmetric Key Cryptography

M S Vilkhu

16-21 Sep 24

Symmetric Key Cryptography

- **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 **publickey encryption in the 1970s**.

- It remains by far the most **widely used** of the two types of encryption.

- Approach

- Study some of the of symmetric ciphers.

- **look at a general model** for the symmetric encryption process;

- Help to understand the **context within which the algorithms** are used.

- Next, we examine a **variety of algorithms in use before the computer era**.

- Finally, we look briefly at a different approach known as **steganography**.

- Study two most widely used symmetric cipher: **DES and AES**

Basic Terms

- **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

- **Cryptology** Both cryptography and cryptanalysis

- **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

Basic Terms

- **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

- **Code** An algorithm for transforming an intelligible message into an unintelligible one using a code-book

Symmetric Cypher Model

Decryption algorithm: This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext.
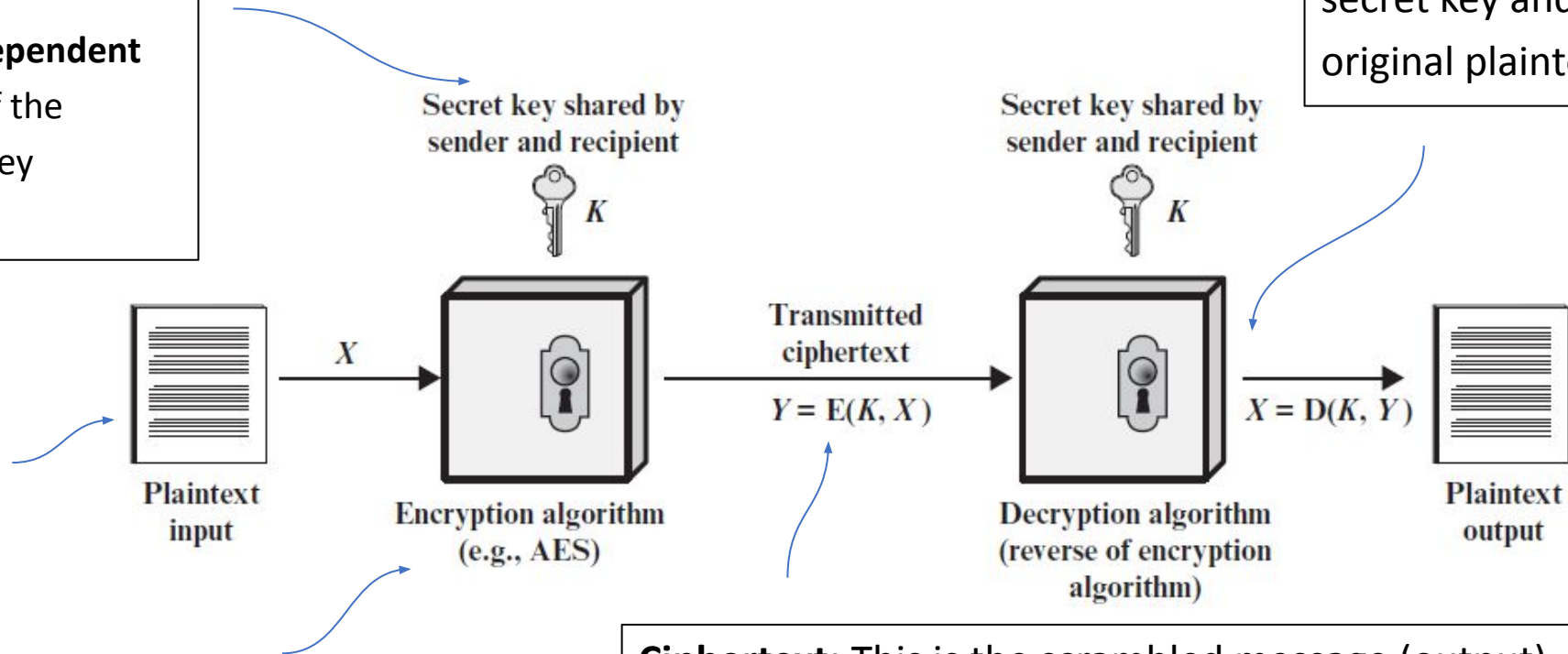
Secret key: The secret key is also input to the **encryption algorithm**.
The key is a value **independent** of the plaintext and of the algorithm. Different key different output

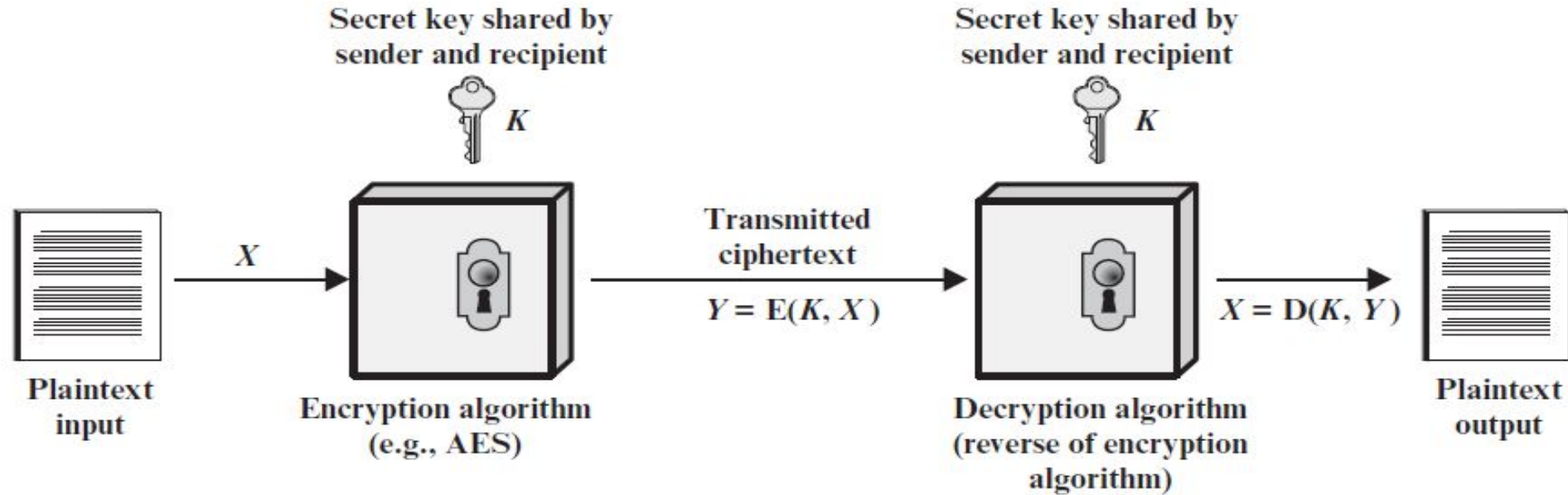**Plaintext**: This is the original intelligible message or data input to algo.

Secret key shared by sender and recipient

K

Secret key shared by sender and recipient

K

Plaintext input

X

Encryption algorithm (e.g., AES)

Transmitted ciphertext

$Y = E(K, X)$

Decryption algorithm (reverse of encryption algorithm)

$X = D(K, Y)$

Plaintext output

Encryption algorithm:
The encryption algorithm performs transformation

Ciphertext: This is the scrambled message (output). depends on the plaintext and the secret key.
For a given message, two different keys will produce two different ciphertexts. The ciphertext is an apparently random stream of data and, as it stands, is unintelligible.

5

Symmetric Cypher Model

Secret key shared by sender and recipient

K

Secret key shared by sender and recipient

K

Plaintext input

X

Transmitted ciphertext

$Y = E(K, X)$

$X = D(K, Y)$

Plaintext output

Encryption algorithm (e.g., AES)

Decryption algorithm (reverse of encryption algorithm)

5 components

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

Symmetric Cypher Model

- **Plaintext**: This is the original intelligible message or data input to algo.

- **Encryption algorithm**: The encryption algorithm performs transformation

- **Secret key**: The secret key is also **input** to the **encryption algorithm**.

  - The key is a value **independent** of the plaintext and of the algorithm.

  - The algorithm will produce a **different output depending** on **the specific key** being used at the time.
    The **exact substitutions and transformations** performed by the algorithm **depend on the key**.

- **Ciphertext**: This is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different ciphertexts. The ciphertext is an apparently random stream of data and, as it stands, is unintelligible.

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

symmetric encryption: Two requirements

- **Two requirements** for secure use of symmetric encryption:

– **A strong encryption algorithm**

we would like the algorithm to be such that an opponent who knows the algorithm and has access to one or more ciphertexts would be unable to decipher the ciphertext or figure out the key.

– **A secret key known only to sender / receiver**

Obtain copy of key through secure means.

Keep the **key secure**

Algo – known to both user and attacker

Key – to be kept secret

With the use of symmetric encryption, the principal security problem is maintaining the secrecy of the key.

symmetric encryption

- **Algorithms** for symmetric encryption is **not required to be kept secret**

- It means that **chip** can be made with **data encryption algorithms**,

- requirement is to keep the **key secret**

Cryptography

Classification of Cryptography
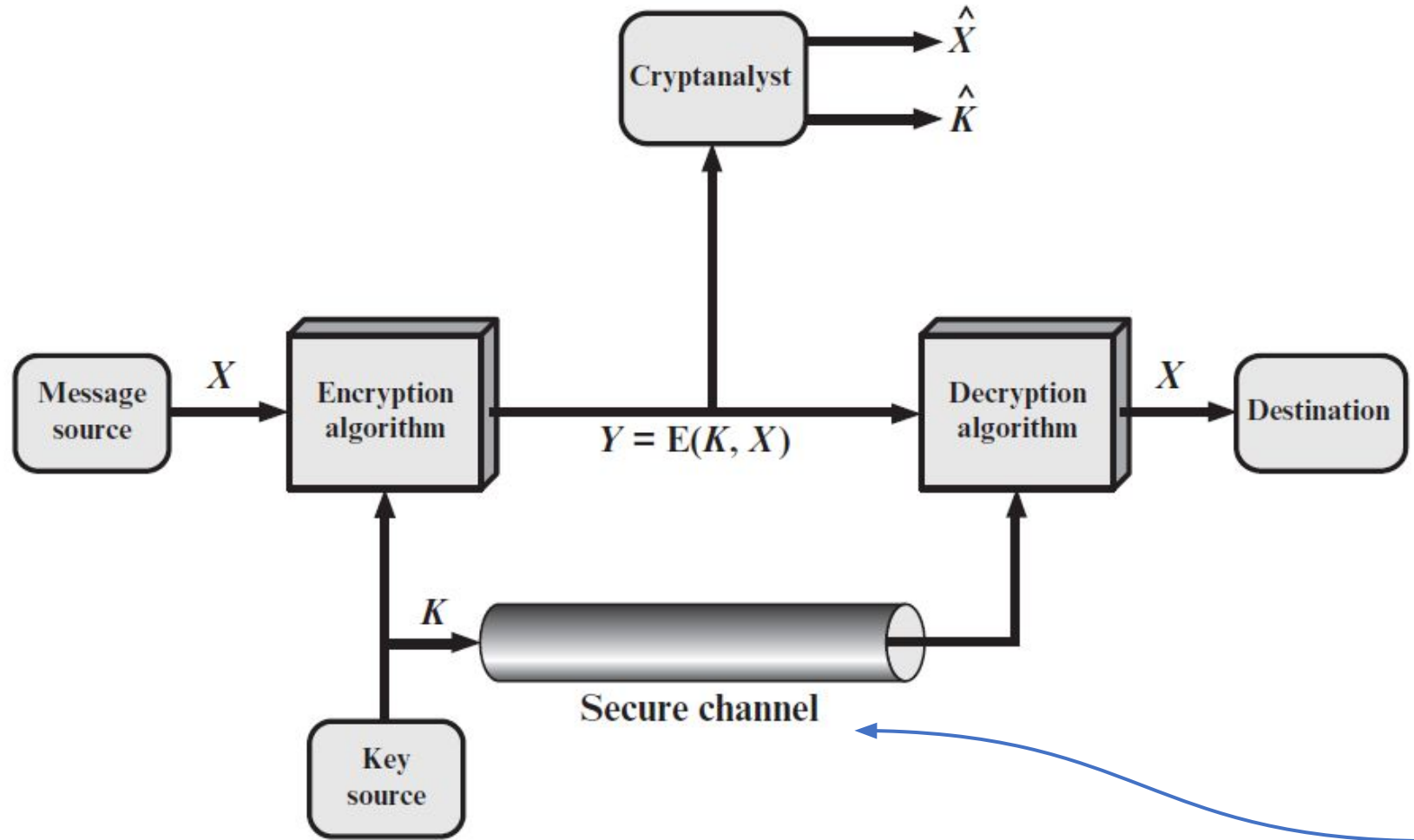## Symmetric Key Cryptography
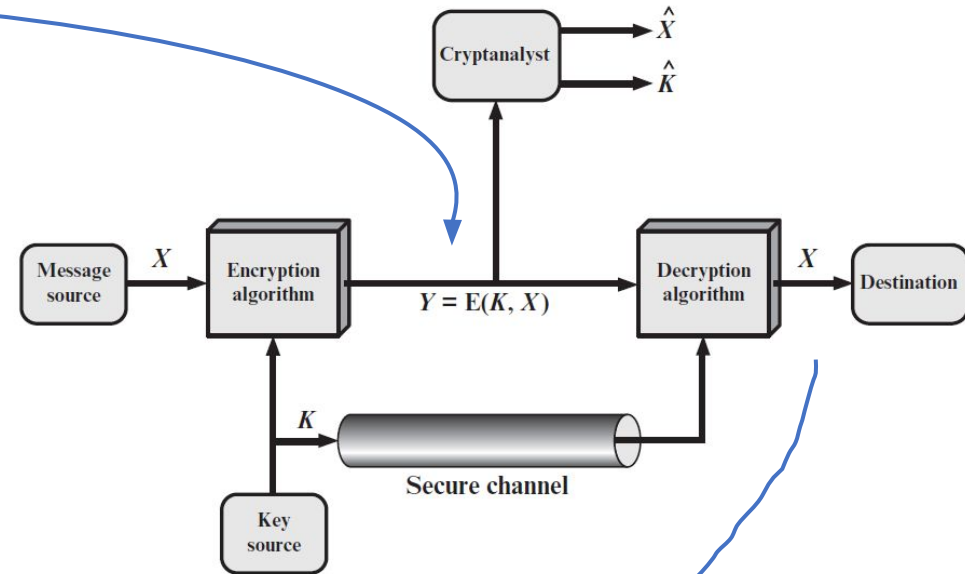
M S Vilkhu

20 Sep 2024(C5)

Symmetric Key Model

Key generated at source should be shared with the destination **through secure channel**

Model

- Y = E (X, K)

- Y is crypto text produced by **encryption algo E** with message X and Key K

- X = D (Y, K)

- X – message, **D decrypt algorithm**, Y is crypto text, K - key

Cryptography Characterized by dimensions

Cryptographic systems are **characterized** along **three** **independent dimensions**:

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

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

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

Cryptography Characterized by dimensions

Cryptographic systems are **characterized** along **three independent dimensions**:

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

All encryption algorithms are based on **two general principles**:

substitution, in which each element in the plaintext (bit, letter, group of bits or letters) **is mapped into another element**, and

transposition, in which **elements in the plaintext are rearranged**.

The fundamental requirement - **no information be lost** (i.e., that all **operations are reversible**).

Most systems, referred to as product systems, involve **multiple stages of substitutions and transpositions**.

Cryptography Characterized by dimensions

Cryptographic systems are **characterized** along **three independent dimensions**:

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

If both sender and receiver use the **same key**, the system is referred to as **symmetric**, single-key, secret-key, or conventional encryption.

If the sender and receiver use **different keys**, the system is referred to as **asymmetric**, two-key, or public-key encryption.

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

A **block cipher** processes the input **one block of elements** at a time, producing an output block for each input block.

A **stream cipher** processes the input elements **continuously**, producing output **one element at a time**, as it goes along.

Break the code

- With help of symmetric algorithm and the cyphertext – is it possible to decrypt the message (plaintext)?

- Algo – is know

- Cypher text – can be captured or read while the message is transmitted

- Is it possible to determine   plain text?

Break the code

- An opponent, **observing Y** but not having access to K or X,

- may attempt to recover X or K or both X and K.

- assumed opponent knows the encryption (E) and decryption (D) algorithms.

- **Two scenarios**

- If Interest & focus is **X particular message** then efforts to estimate plain text X

- If opponent is interested in being able to read **future messages -** an attempt is made to recover **K** by generating an estimate K
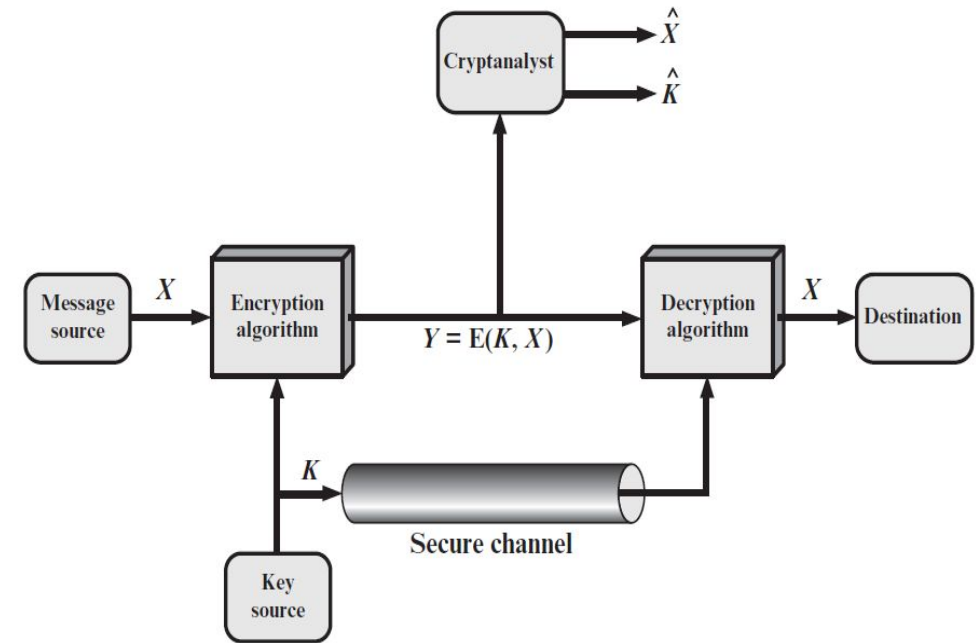
Cryptanalysis and Brute-Force Attack

Cryptanalysis and Brute-Force Attack

- What is Cryptanalysis?

- What is Brute-Force Attack

- Difference

- **objective** of attacking an encryption system is to **recover the key** in use rather than simply to recover the plaintext of a single ciphertext.

- **two general approaches to attacking** a conventional encryption scheme:

- **Cryptanalysis**:

- **Brute-force attack**:

Cryptanalysis and Brute-Force Attack

- **Cryptanalysis**: Cryptanalytic attacks
    - rely on the **nature of the algorithm**
    - some knowledge of the general **characteristics of the plaintext** or
    - even some **sample plaintext–ciphertext pairs**.

- This type of attack exploits the **characteristics of the algorithm** to attempt to deduce a
    - **specific plaintext** or
    - to **deduce the key** used.

Cryptanalysis and Brute-Force Attack

- **Cryptanalysis**: Cryptanalytic attacks
  - rely on the **nature of the algorithm**
  - some knowledge of the general **characteristics of the plaintext** or
  - even some **sample plaintext–ciphertext pairs**.
- This type of attack exploits the **characteristics of the algorithm** to attempt to deduce a **specific plaintext** or to **deduce the key** being used.

- **Brute-force attack:** The attacker **tries every possible key** on a piece of ciphertext until an **intelligible translation** into plaintext is obtained.
- **On average**, half of all possible keys must be tried to achieve success.

If either type of **attack succeeds** in deducing the key, the effect is **catastrophic**:
All future and past messages encrypted with that key are compromised.

Cryptanalysis and Brute-Force Attack

Aspect	Cryptanalysis	Brute Force Attack
Definition	Analyzing cryptographic systems to find **weaknesses or vulnerabilities**.	Systematically trying **every possible** key or password.
Method	Uses **analytical techniques**, such **as pattern recognition**, **statistical analysis**, and **algebraic methods.**	**Exhaustively** tests all possible keys or passwords.
Goal	To find a more efficient way to decrypt data or discover the key.	To **find the correct key** or password through exhaustive search.
Efficiency	Can be more **efficient if vulnerabilities are found**; may reduce the amount of work needed.	Can be **very inefficient**, especially with strong encryption, as it involves testing all possibilities.
Knowledge Required	Requires understanding of the cryptographic algorithm and its **potential weaknesses**.	**No need for knowledge about the algorithm**, just a systematic approach to trying all possible keys.
Examples of Techniques	**Differential cryptanalysis, linear cryptanalysis, known plaintext attacks.**	Trying **every possible key for** a given encryption algorithm, e.g., **a 128-bit key requires 2^{128} attempts**.
Computational Demand	Can vary widely **depending on the weakness exploited;** sometimes **less computational power is needed compared to brute force**.	**High computational demand**, especially for strong encryption with large key sizes.
Practicality	Effective if **weaknesses in the encryption are found**; can be feasible with sophisticated techniques.	Often **impractical for strong encryption** due to the vast number of combinations.

Cryptography

Classification of Cryptography
Symmetric Key Cryptography

M S Vilkhu

21 Sep 2024(C1/ C3/c5)

Cryptanalysis : Methods

1. **Pattern Recognition:**

2. **Statistical Analysis:**

3. **Algebraic Methods:**

Cryptanalysis : Methods

1. **Pattern Recognition:**

- **Definition**:
- The process of identifying **regularities**, **structures**, or **repeating** elements within a cryptographic message or encrypted data.

- In cryptanalysis, this often involves looking for **repeated sequences, common phrases, or structural patterns, visual pattern** that can reveal information about the encryption method or the plaintext.
- to infer **plaintext or encryption rules**.

- **Application**:
- For example, **in a substitution cipher**, the **frequency** **of letter** or **word patterns** in the ciphertext can be analyzed to guess the substitution mappings.

It's more **qualitative** and relies on recognizing **specific features** or **sequences**.

Cryptanalysis : Methods

2. Statistical Analysis:

Definition: The application of statistical methods to **analyze the frequency and distribution of symbols or patterns** in ciphertext.

This can help **identify anomalies or deviations** from **expected distributions** that can be **exploited to break the cipher**.

Application: In classical cryptography, **frequency analysis** involves studying the **frequency of letters** or groups of letters in ciphertext.

For instance, in **English text, the letter 'E' is the most common**, so an analyst might look for the most frequent letters in the ciphertext and hypothesize that they correspond to 'E' or other common letters.

Focuses on **quantitative analysis** of the **frequency and distribution of symbols**.

It involves applying **statistical methods** to detect **deviations from expected patterns** and **deduce information about the encryption**.

Cryptanalysis : Methods

3. **Algebraic Methods:**

Definition: Techniques that **use algebraic structures and equations** to analyze and solve cryptographic problems.

This involves **applying mathematical** operations and theories to **deduce the encryption keys** or to **understand the transformation functions** used in encryption.

Application:

In the case of **linear cryptanalysis**, algebraic techniques are used to **create linear approximations** of the encryption function.

For **block ciphers** like **DES**, algebraic methods might involve **solving systems of linear equations to determine the key.**

Cryptanalysis : Methods

Aspect	Pattern Analysis	Statistical Analysis
Focus	Repetitions and patterns in the ciphertext	Frequency distribution of letters or letter groups

For instance, the word
MI LI TA RY
will always produce the same ciphertext letter in **the first and third** positions regardless of the keywords used.

Patterns like these can be catalogued and matched against single-letter repeats in the ciphertext.

Analyzes the **frequency** of letters, digraphs, or other elements in the ciphertext based on known statistical properties of the language in the plaintext (e.g., in English, the letter "E" is the most frequent, followed by "T" and "A").

if "X" appears most frequently in the ciphertext, it might correspond to "E" in English since "E" is the most common letter in English.

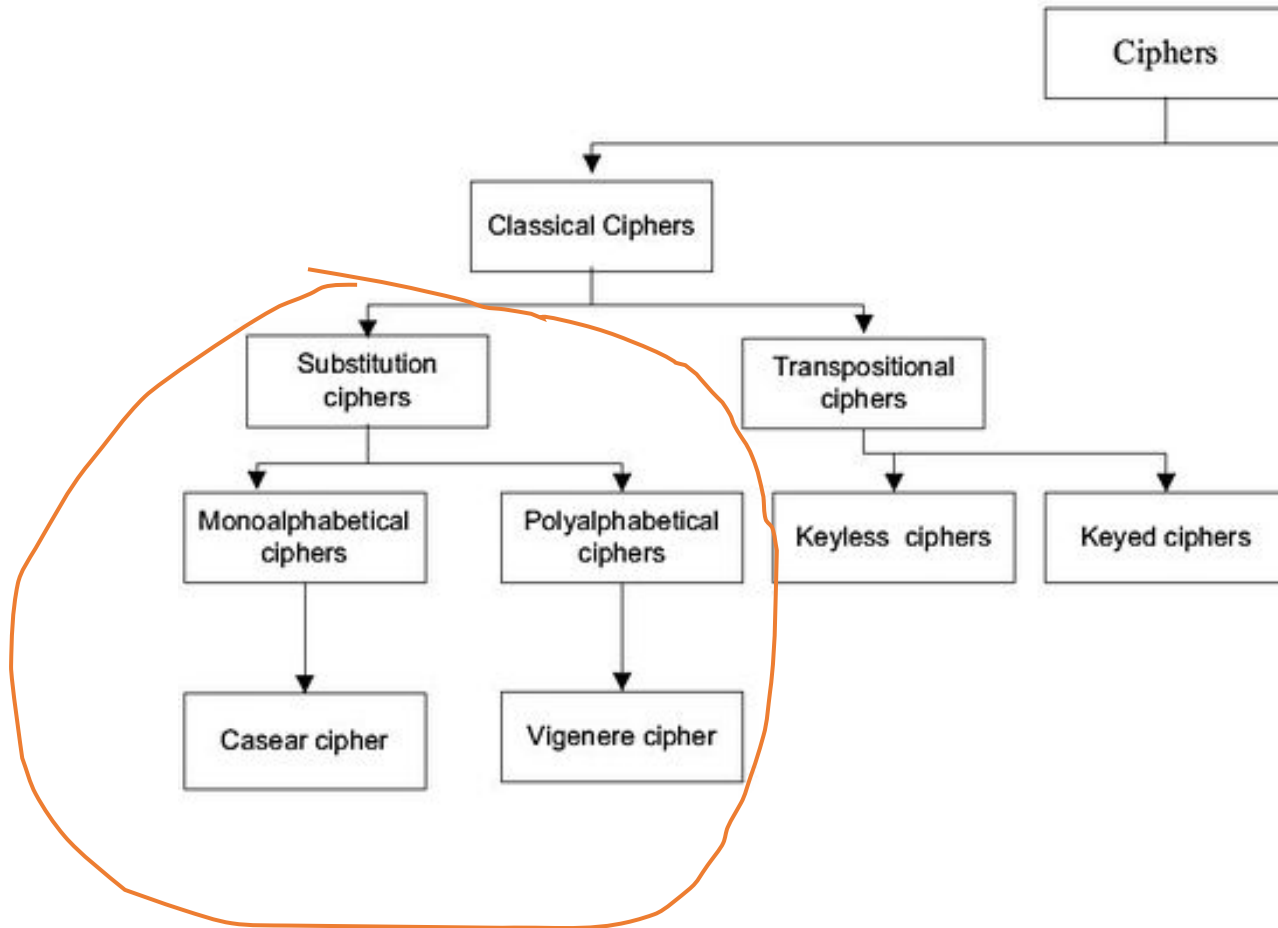# Symmetric Key Cryptography techniques

Symmetric Key Cryptography techniques

- examine a sampling of what might be called **classical encryption techniques.**

- two basic building blocks of all encryption techniques
    - **Substitution Techniques**
    - **Transposition techniques**
    - There are systems which **combine both**

study of these techniques enables us

- to illustrate the **basic approaches** to symmetric encryption used today and

- the types of **cryptanalytic attacks** that must be anticipated.

Classification

Symmetric Key Cryptography techniques

- **Substitution Techniques**

- 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.

- **replacing each element** of the plaintext with **another element** according to a fixed system or rule.

- **The idea** - to **disguise the original text** by substituting each letter or symbol with another.

Symmetric Key Cryptography techniques

- **Substitution Techniques**

Monoalphabetic Ciphers

- **Caesar Cipher**

- **Atbash Cipher**

- **Playfair Cipher**

Polyalphabetic ciphers

- **The Vigenère cipher**

Symmetric Key Cryptography techniques

- **Substitution Techniques**

- **Caesar Cipher**

- The Caesar cipher is a simple substitution cipher where each letter in the plaintext is **shifted a fixed number** of places down or up the alphabet.

- 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

  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

Symmetric Key Cryptography techniques

- **Substitution Techniques**

- **Caesar Cipher**

    Plaintext: HELLO

    Shift: 3

    Ciphertext: KHOOR

    In this example, each letter in "HELLO" is shifted by 3 positions in the alphabet

    H → K

    E → H

    L → O

    L → O   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

    O → R   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

Symmetric Key Cryptography techniques

- **Substitution Techniques**

- **Caesar Cipher**

Mathematically

$C = \text{E}(3, p) = (p + 3) \bmod 26$ where p- plaintext, c ciphertext

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

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

k takes the value from 1 to 25

Decrypt algorthym

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

Symmetric Key Cryptography techniques

- **Substitution Techniques**

- **Caesar Cipher**

If it is known that a given ciphertext is a **Caesar cipher**, then a **brute-force cryptanalysis** is easily performed:

simply try all the 25 possible keys. shows the results of applying this strategy to the example ciphertext.

.

Three important characteristics of this problem **enabled us to use a bruteforce cryptanalysis:**

1. The encryption and decryption **algorithms are known.**

2. There are only **25 keys to try**.

3. The language of the **plaintext is known** and easily **recognizable**.

Symmetric Key Cryptography techniques

- **Substitution Techniques**

- **Caesar Cipher**

Very important

3. The language of the **plaintext is known** and easily **recognizable**.

If the **file is compressed** and then encrypted, then **recognizing the** plaintext is difficult

Symmetric Key Cryptography techniques

- **Substitution Techniques**
- **Caesar Cipher**

Very important

3. The language of the **plaintext is known** and easily **recognizable**.

If the **file is compressed** and then encrypted, then **recognizing the plaintext is difficult**

File compression is the process of **reducing the size** of a file by encoding its data more efficiently, typically by **eliminating redundancies, re-encoding repeated patterns, or using mathematical algorithms.** The goal of compression is to make files smaller, so they use less storage space and can be transmitted more quickly over networks

Symmetric Key Cryptography techniques

- **Substitution Techniques**

- **Atbash Cipher**

- The Atbash cipher is a substitution cipher where **each letter is mapped to its reverse** in the alphabet.

    Plaintext: HELLO

    Ciphertext: SVOOL

    In this example, each letter in "HELLO" is replaced with its reverse:

    H → S

    E → V

    L → O

    L → O

    O → L

Symmetric Key Cryptography techniques

- **Substitution Techniques**

- **Monoalphabetic Ciphers**

- With **only 25 possible keys**, the Caesar cipher is far from secure.

- **increase in the key space** can be achieved by **allowing an arbitrary substitution**.

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

line of attack.
If the cryptanalyst knows the nature of the plaintext (e.g., noncompressed English text), then the analyst can exploit the **regularities of the language**.

Symmetric Key Cryptography techniques

- **Substitution Techniques**

- **Monoalphabetic Ciphers**

- **Variation to Caesar Cipher**

- **assignment** for the 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

- instead, the "cipher" line can be any **permutation of the 26 alphabetic** characters,

- then there are 26! or greater than 4 x 10^{26} possible keys

Permutation.
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, if S = {a, b, c},
six permutations of S
For n, there are n! combinations

Cryptoanalysis and Regularities of the language

- **Regularities of the language**.

- **Regularities** of a language refer to the **consistent patterns** and **structures found** within a language that can be **exploited** in various fields, including **cryptography,** linguistics, and natural language processing.

- Understanding these regularities helps in areas such as **cryptanalysis**, text analysis, and language modeling.

Cryptoanalysis and Regularities of the language

Regularities of the language.

1. **Frequency of Letters and Words** - certain letters appear more frequently than others

2. **Common Letter Combinations** -Certain pairs (bigrams) or triplets (trigrams) of letters appear frequently in text. For instance, 'TH', 'HE', and 'ING

3. **Morphology** -Languages have regular patterns for creating new words or altering word forms   - ed for past tense,

4. **Grammar and Syntax** -regular syntactic rules governing sentence structure

5. **Patterns in Punctuation**

6. **Textual Cohesion and Coherence** – structured, different parts of a text are linked together

Cryptoanalysis and Regularities of the language

- **Substitution Techniques**

- **Monoalphabetic Ciphers**

- Cypher text to be solved –

- UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZVUEPHZHMDZSHZOWSFP APPDTSVPQUZWYMXUZUHSXEPYEPOPDZSZUFPOMB**ZWP**FUPZHMDJUDTMOHMQ

- Relative frequency of letters.

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				

Cryptoanalysis and Regularities of the language

- **Substitution Techniques**

- **Monoalphabetic Ciphers**

- **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}.**

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				
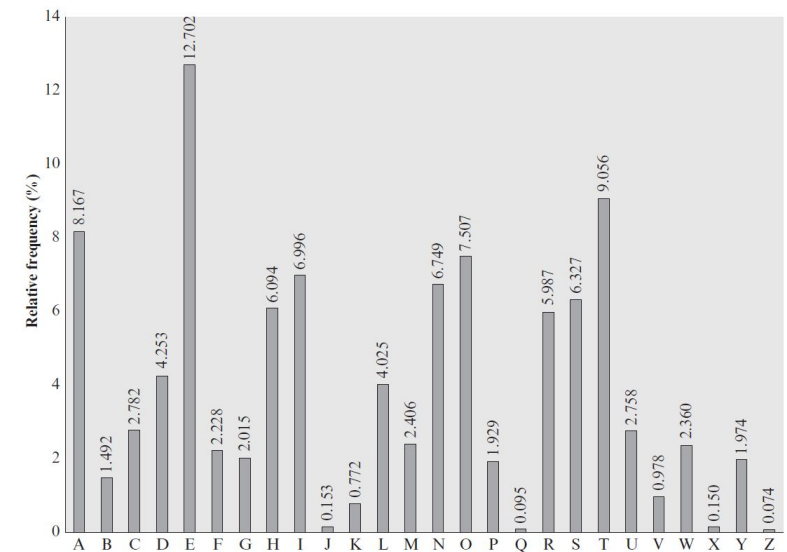
Cryptoanalysis and Regularities of the language

- **Substitution Techniques**

- **Monoalphabetic Ciphers**

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								

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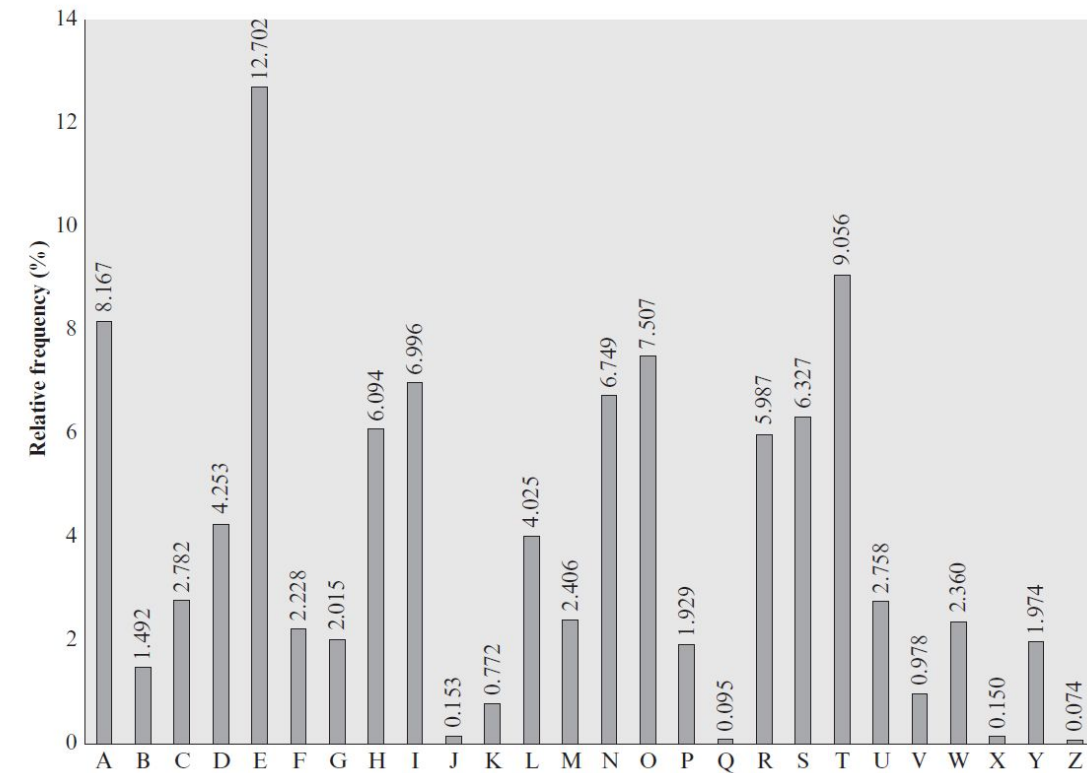- lowest frequencies (**namely, A, B, G, Y, I, J**) are likely included in the □ set {**b, j, k, q, v, x, z**}.

Cryptoanalysis and Regularities of the language

- **Substitution Techniques**

- **Monoalphabetic Ciphers**

- powerful tool is to look at the for **Continued analysis** of frequencies **plus trial and error** should easily yield a

- Solution sequency of **two-letter combinations**, known as **digrams**

- 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**.

- Then look at frequency of **trigram** ZWP

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

Cryptoanalysis and Regularities of the language

- **Substitution Techniques**

- **Monoalphabetic Ciphers**

Ciphertext

UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ

```
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
```

Plain text

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

- **Continued analysis** of frequencies **plus trial and error** should easily yield a
- Solution sequency of **two-letter combinations**, known as **digrams**
- 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.**
- Then look at frequency of trigram ZWP

Cryptoanalysis and Regularities of the language

- **Substitution Techniques**

- **Monoalphabetic Ciphers**

- For Cipher text

UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZVUEPHZHMDZSHZOWSFPAP
PDTSVPQUZWYMXUZUHSXEPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ

- Plain text is

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

Cryptoanalysis and Regularities of the language

- **Substitution Techniques**

- **Monoalphabetic Ciphers**

- Monoalphabetic ciphers are **easy to break** because they **reflect the frequency** data of the original alphabet.

- A **countermeasure** is to provide **multiple substitutes**, known as **homophones**, for a single letter.

- For example, the letter **e** could be assigned a **number of different cipher symbols,** such as 16, 74, 35, and 21, with each homophone assigned to a letter in **rotation or randomly**.

- If the

- number of symbols assigned to each letter is **proportional** to the **relative frequency** of that letter,

then **single-letter frequency** information is completely **obliterated**.

Cryptoanalysis and Regularities of the language

- **Substitution Techniques**

- **Monoalphabetic Ciphers**

- The great mathematician **Carl Friedrich Gauss** believed that he had devised an **unbreakable cipher using homophones**.
  - However, even with **homophones**, each **element of plaintext affects only one element of ciphertext,** and
  - **multiple-letter patterns** (e.g., **digram frequencies**) **still survive** in the ciphertext,

- making cryptanalysis relatively straightforward.

- **Two principal methods** are used in **substitution ciphers to lessen the extent** to which the **structure of the plaintext survives in the ciphertext**:
  - One approach is to **encrypt multiple letters of plaintext**, and
  - the other is to **use multiple cipher alphabets**.

Symmetric Key Cryptography techniques

- **Substitution Techniques**

- **Monoalphabetic Ciphers**

- **Two principal methods** are used in **substitution ciphers to lessen the extent** to which the **structure of the plaintext survives in the ciphertext**:
    - One approach is to **encrypt multiple letters of plaintext**, and
    - the other is to **use multiple cipher alphabets**.

- Playfair Cipher

Symmetric Key Cryptography techniques

- **Substitution Techniques**

- **Playfair Cipher**

- The best-known **multiple-letter encryption** cipher is the Playfair,

- which treats **digrams** in the plaintext **as single units** and translates these units into **ciphertext digrams**

- invented by **Charles Wheatstone in 1854** and popularized by Lord Playfair.

- The Playfair cipher is **more complex than a monoalphabetic substitution** cipher and offers **better security**.

- based on 5 x 5 matrix of letters

- constructed using a keyword.

- Here is an example, step by step method

Symmetric Key Cryptography techniques

- **Substitution Techniques**

- **Playfair Cipher**

Step 1.

Create a **5x5 Key Square**: The first step is to generate a 5x5 grid of letters using a keyword (**minus the duplicate**). (left to right and top to bottom)

The **keyword** is written into the grid first, without repeating letters. (Left to right)

After the **keyword, the rest of the alphabet is filled in**, omitting the letter "J" (which is combined with "I" to fit in the 25-letter grid)

Keyword - MONARCHY

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

Symmetric Key Cryptography techniques

- **Substitution Techniques**
- **Playfair Cipher**

Step 2.

Prepare the Plaintext: The plaintext is **divided into pairs** of letters (**digraphs**).

If a pair contains **two identical letters**, **or** if there's an **odd number of letters**, an extra filler letter like **"X" is added**.

"I" and "J" are treated as the same letter.

Example:

Plaintext: BALLOON

Split into digraphs: BA LL OO N

After handling **double letters** and **odd length**: BA LX LO ON

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

Symmetric Key Cryptography techniques

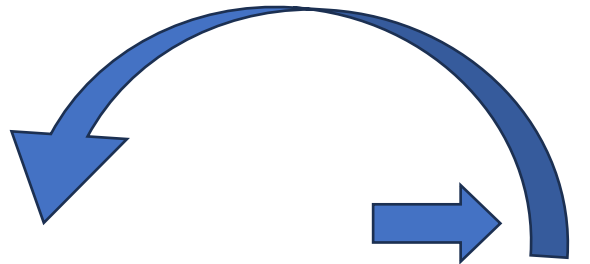- **Substitution Techniques**

- **Playfair Cipher**

Step 3.

Encryption Rules:

Repeating plaintext letters that are in the same pair are separated with a filler letter, such as x,

balloon □ treated as **BA LX LO ON**

Rules

Same row. 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**

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

Symmetric Key Cryptography techniques

- **Substitution Techniques**

- **Playfair Cipher**

Same column: 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.**

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

Different row and column:

letters **form a rectangle**, replace them with the letters on **the same row**, but at the **opposite corners of the rectangle**.

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 □ **BP** and

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

ea □ **IM** (or JM, as the encipherer wishes).

If the

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

Symmetric Key Cryptography techniques

- **Substitution Techniques**

- **Playfair Cipher**

Step 3.

Encryption Rules:

Repeating plaintext letters that are in the same pair are separated with a filler letter, such as x,

balloon □ treated as **BA LX LO ON**

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

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

Symmetric Key Cryptography techniques

- **Substitution Techniques**

- **Playfair Cipher**

Step 4.

Encrypt the Digraphs

Digraph 1: BA

B is in row 2, **column 4**.

A is in row 1, **column 4**.

Since they are in the **same column**, move down:

B -> I, A -> B.

Encrypted digraph: IB

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

Symmetric Key Cryptography techniques

- **Substitution Techniques**
- **Playfair Cipher**

Step 4.

Encrypt the Digraphs

Digraph 2:

L is in row 4, column 1.

X is in row 5, column 4.

They form a **rectangle**, so swap the columns: **L -> S, X -> U. Encrypted diagram SU**

Digraph 3:

LO is in row 4, column 1.

O is in row 1, column 2.

They form a **rectangle**, so swap the columns: **L -> P, O -> M. Encrypted digraph: PM**

Digraph 4: ON

O is in row 1, column 2.

N is in row 1, column 3.

Since they are in the **same row**, move right one position: **O -> N, N -> A. Encrypted digraph: NA**

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

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

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

Symmetric Key Cryptography techniques

- **Substitution Techniques**

- **Playfair Cipher**

- Final Ciphertext:

- After encrypting all the digraphs, the final ciphertext for

- **BALLOON** becomes :**IBSU PMNA**

Symmetric Key Cryptography techniques

- **Substitution Techniques**

- **Playfair Cipher**

- **Decryption:**

- Decryption follows the same **steps but in reverse**:

- If the digraph letters are in the same row, move left one position.

- If they are in the same column, move up one position.

- If they form a rectangle, reverse the corner swapping process.

The Playfair cipher provides **greater security** than monoalphabetic ciphers because it operates on digraphs, making it harder to perform frequency analysis. However, with modern techniques, it can still be broken relatively easily compared to more advanced ciphers.

Symmetric Key Cryptography techniques

- **Substitution Techniques**

- **Playfair Cipher**

- <mark>**identification** of **individual digrams is more difficult**</mark>.

- the **relative frequencies** of individual letters exhibit a **much greater range** than that of digrams, **making frequency analysis much more difficult**.

- Playfair cipher was for a long time **considered unbreakable**.

- It was used as the standard **field system** by the **British Army** in **World War I** and enjoyed considerable use by the U.S. Army and other Allied forces during **World War II.**

- **Strength of the Playfair Cipher**

- The Playfair cipher is a **great advance over simple monoalphabetic cipher**s. For one thing, whereas there are **only 26 letters, there are 26 * 26 = 676 digrams**

- **easy to break**, -- much of the **structure of the plaintext** language is intact.

Thank You