UCSLAB
Ubiquitous Computing & Security Laboratory

Chapter 2: Classical Encryption Techniques

Presented by:
Abir EL.
03/16/2021
Professor. 박종혁
Cryptography and information Security

Table of Content:

Classical Encryption Techniques

What is Encryption?

Encryption, is the process of changing information in such a way as to make it unreadable by anyone except those possessing special knowledge (usually referred to as a "key") that allows them to change the information back to its original, readable form.

Goals of this chapter:

- Introduce basic concepts and classical terminologies and encryption technologies.
- An introduction to the upcoming chapters.

Classical Encryption Techniques

Basic Terminology and Key words:

- **Plaintext:** Refers to the original text or message to be encrypted.
- **Ciphertext:** The encrypted message.
- **Enciphering** or **Encryption**: The process of converting plaintext into a ciphertext.
- **Deciphering** or **Decryption**: The process of decoding the ciphertext and retrieving the original plain text.
- **Encryption algorithms**: a pseudocode based on mathematical equations to perform encryption. Usually requires two inputs; the **Plaintext** and the **Secret Key.**
- **Decryption algorithm**: Used to perform the decryption. Usually requires two inputs as well; **Ciphertext** and **Secret Key**.
- **Secret Key**: A special key used for encryption and decryption, known as well as **Symmetric Key**.

Classical Encryption Techniques

Basic Terminology and Key words:

- **Cipher** or **Cryptographic system**: Refers to the scheme used for encryption and decryption.
- **Cryptography**: The science that studies and analyze ciphers.
- **Cryptanalysis**: Science of studying attacks against cryptographic systems.
- **Cryptology**: The science that merge both Cryptography and Cryptanalysis.
- **Symmetric Cipher**: Using the same key for encryption and decryption such as:
  - Block Cipher: Encrypts a block of plaintext at a time (usually 64 or 128 bits).
- **Asymmetric Cipher**: Using different keys for encryption and decryption phases.

Classical Encryption Techniques

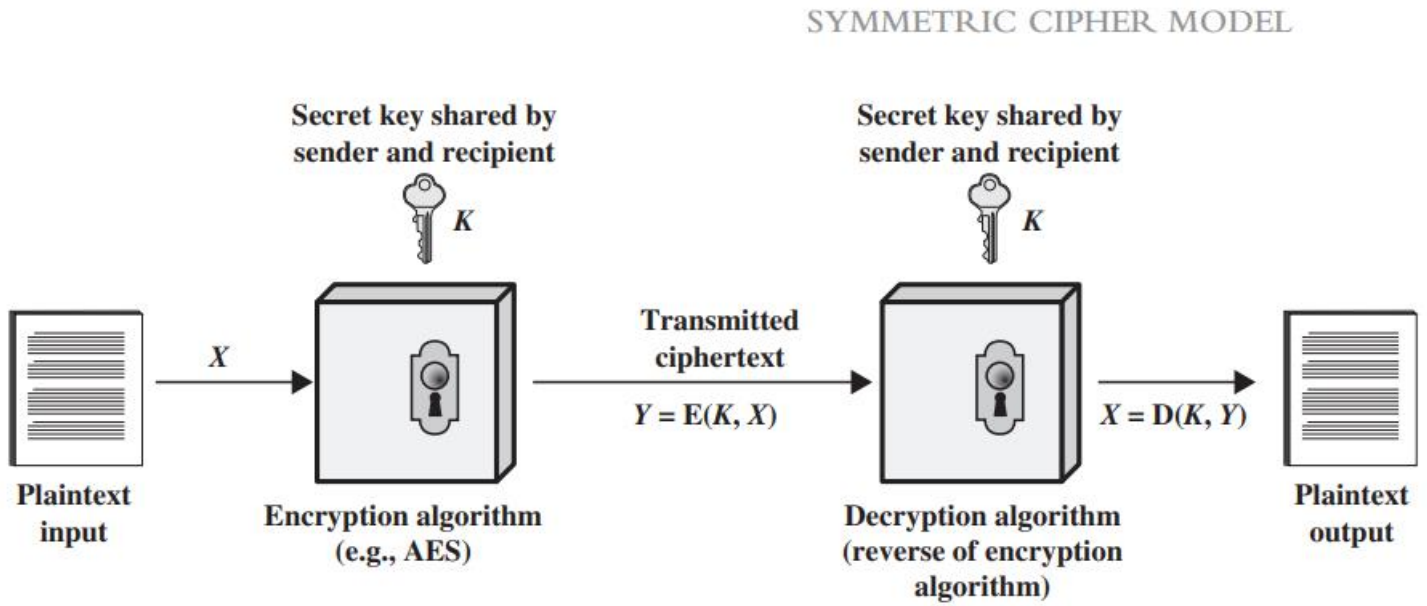
1. Symmetric Cipher model:

- The symmetric encryption technique uses the same key to encrypted and decrypt the plaintext.
- The symmetric cypher model consist of five elements:
  - Plaintext.
  - Encryption algorithm.
  - Secret Key.
  - Ciphertext.
  - Decryption algorithm.
- The security level of the symmetric encryption depends on the **secrecy** of the **key**, and NOT the secrecy of the algorithm.

Classical Encryption Techniques

1. Symmetric Cipher model:

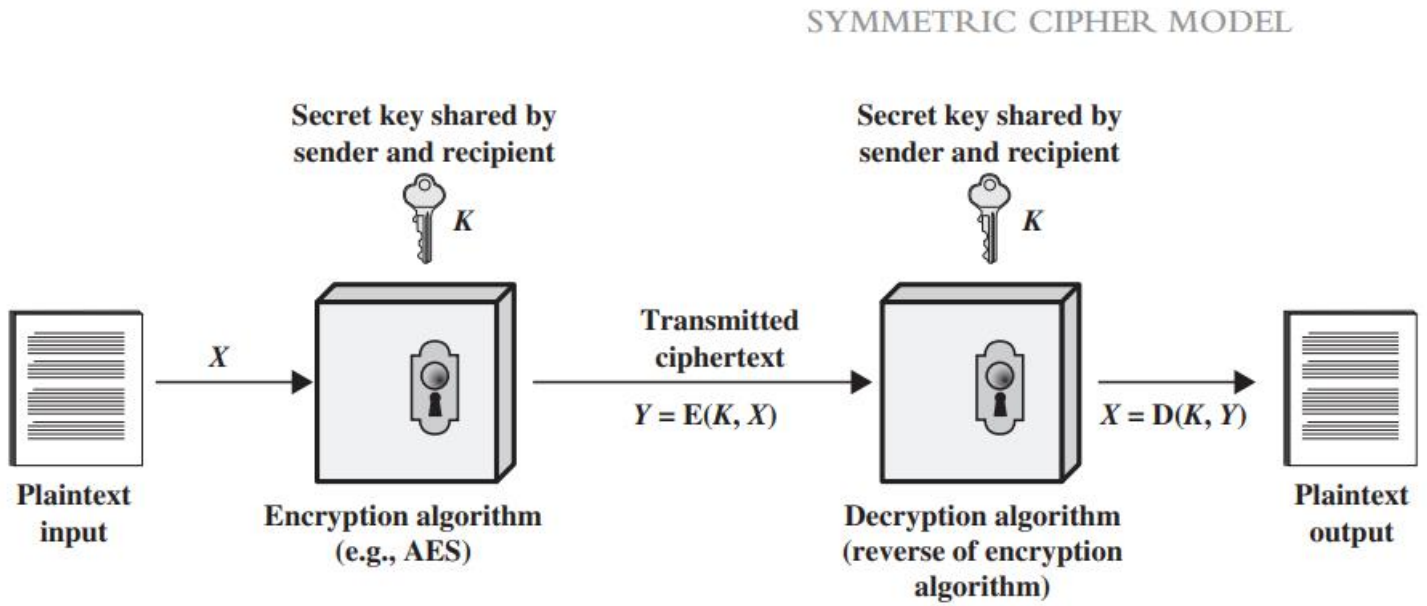
- **Plaintext** is the original message or data that will be fed to the encryption algorithm as an input.
- **Encryption algorithm** performs various substitutions and transformations on the plaintext.
- **Secret key** is a value independent of the plaintext and of the algorithm. The exact substitutions and transformations performed by the algorithm depend on the key.



Classical Encryption Techniques

1. Symmetric Cipher model:

- Ciphertext is the unreadable message produced as output. It depends on the plain text and the secret key.
- Decryption algorithm takes the cipher text and the secret key to retrieve the original text



Classical Encryption Techniques

1. **Symmetric Cipher model:** Mathematical representation

- Mathematically, the equation related to the encryption algorithm can be represented as follows

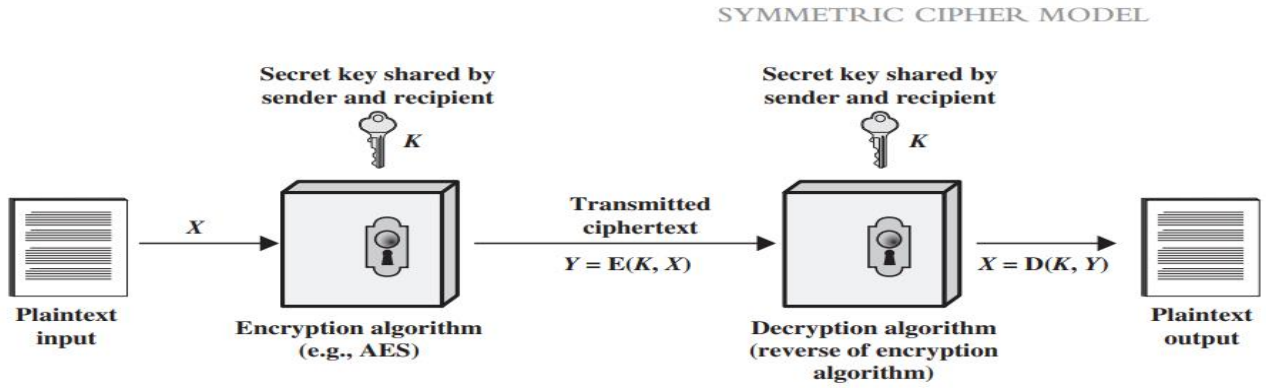
$$Y = E(K, X)$$

Where Y = cipher text, E = encryption, K = Secret shared key, X = Plaintext

- The equation related to the decryption can as well be represented as follows:

$$D = E(K, X)$$

- Where D = Decryption
- Some examples of symmetric encryption includes Data Encryption Standard (DES), Advanced Encryption Standard (AES), and BLOWFISH



Classical Encryption Techniques

1. Symmetric Cipher model: Advantages and disadvantages

- **Advantage:**
- Symmetric key is faster than asymmetric key cryptography.
- Same key is used for encryption and decryption, receiver cannot decrypt data without key (shared by the sender)
- Symmetric key achieves the authentication principle because it checks receiver's identity.
- System resources are less utilized.

- **Disadvantage:**
- Once key is diffused, transmitted data is not secure anymore and can easily be cracked.
- In symmetric key cryptography, key MUST be shared first between sender and receiver and then message is transferred.

Classical Encryption Techniques

2. Substitution technique

Substitution technique is a classical encryption technique where the characters present in the original message are replaced by other characters or numbers or symbols. If the plain text (original message) is considered as the string of bits, then the substitution technique would replace bit pattern of plain text with the bit pattern of cipher text. The substitution techniques can be explained as follows:

- **Caesar Cipher.**
- **Monoalphabetic Cipher.**
- **Polyalphabetic Cipher.**
- **Playfair Cipher.**
- **One-Time Pad.**
- **Hill Cipher.**

Classical Encryption Techniques

2. Substitution technique: Caesar Cipher

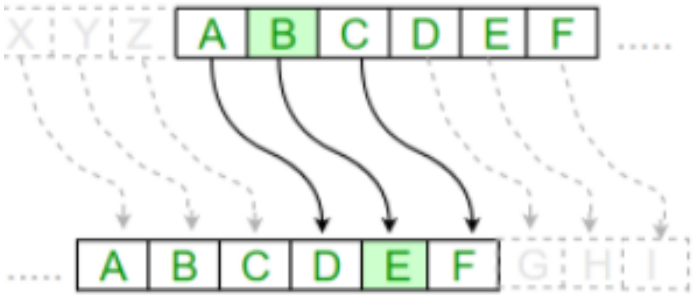
- The Caesar Cipher technique is one of the earliest and simplest method of encryption technique. each letter of a given text is replaced by a letter some fixed number of positions down the alphabet. For example with a shift of 1, A would be replaced by B, B would become C, and so on.
- The method is apparently named after Julius Caesar, who apparently used it to communicate with his officials.
- The encryption can be represented using modular arithmetic by first transforming the letters into numbers, according to the scheme, A = 0, B = 1,…, Z = 25. Encryption of a letter by a shift n can be described mathematically as the figure bellow.

$$E_n(x) = (x + n) mod\ 26$$

(Encryption Phase with shift n)

$$D_n(x) = (x - n) mod\ 26$$

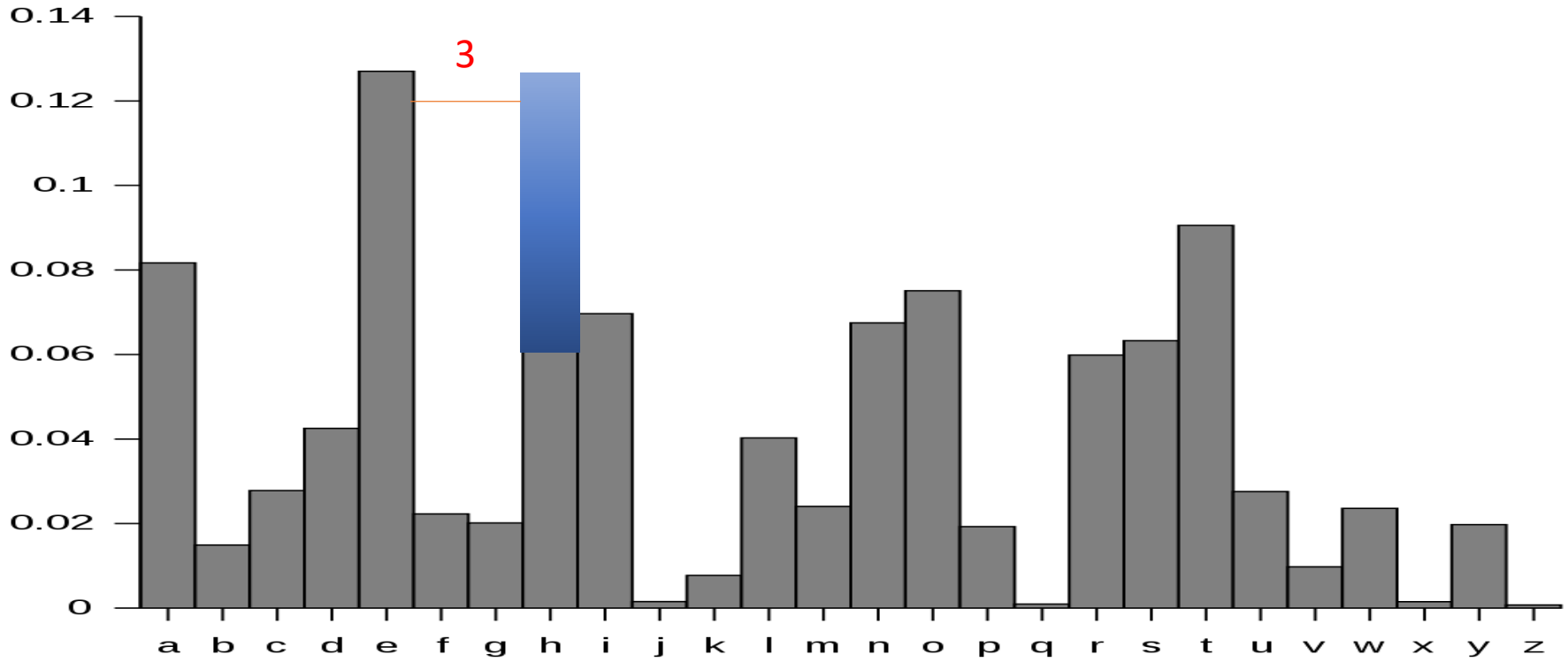
(Decryption Phase with shift n)



Classical Encryption Techniques

2. Substitution technique: Caesar Cipher

- The weakness of this model was published 800 years later by an Arab Mathematician named Al-Kindi. Al-Kindi was capable of breaking the Caesar Cipher by using a clue based on a shared property of the language used in the message, which is the Frequency.



Classical Encryption Techniques

2. Substitution technique: Monoalphabetic Cipher

- Monoalphabetic cipher is a substitution cipher in which for a given key, the cipher alphabet for each plain alphabet is fixed throughout the encryption process. For example, if ‘A’ is encrypted as ‘D’, for any number of occurrence in that plaintext, ‘A’ will always get encrypted to ‘D’.
- The number of possible shifts is 26!, making it much more complicated than Caesar Cipher to break.

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

Classical Encryption Techniques

2. Substitution technique: Polyalphabetic Cipher

- A strong cipher is one which disguises your fingerprint.
- By the mid 15th century, cryptography has advanced to Polyalphabetic Cipher.

Message to Send: Hide the money

Secret Word: RICH

Letter Position: 17 – 8 – 2 – 7

Adding Sequence: Hide the money

17 – 8 – 2 – 7 17 – 8 – 2 7 – 17 – 8 – 2 – 7

Original Position: H i d e t h e m o n e y

7 8 3 4 19 7 4 12 14 13 4 24

17 8 2 7 17 8 2 7 17 8 2 7

Ciphertext: YQFL KPG TFCGF

Classical Encryption Techniques

2. Substitution technique: Polyalphabetic Cipher: The Cipher Disc

- The development of Polyalphabetic Substitution Ciphers was the cryptographers answer to Frequency Analysis.
- The first known polyalphabetic cipher was the Alberti Cipher invented by Leon Battista Alberti in around 1467. He used a mixed alphabet to encrypt the plaintext, but at random points he would change to a different mixed alphabet, indicating the change with an uppercase letter in the ciphertext.
- In order to utilize this cipher, Alberti used a cipher disc to show how plaintext letters are related to ciphertext letters.

Classical Encryption Techniques

2. Substitution technique: Polyalphabetic Cipher

- As an example we shall encrypt the plaintext "leon battista alberti". To keep with the convention of writing ciphertext in uppercase, we shall invert Alberti's own rule, and use lowercase letters to signify the change.

- We start by referencing the starting position of the cipher disc, which in this case is "a" is encrypted as "V", so we start the ciphertext with a lowercase "v". We then encrypt the first few letters as a Caesar Shift, using the ciphertext alphabet given below.
- Plaintext: leonbat
  Ciphertext: vGZJIWVOg...

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

Classical Encryption Techniques

2. Substitution technique: Polyalphabetic Cipher

- The uppercase letters above encrypt the plaintext letters given. The "v" indicates the starting position of the disc, and the "g" indicates that we need to change the position so that "G" is beneath "a". We then get the new ciphertext alphabet.
- Plaintext: ...tistaa...
  Ciphertext: ...gZOYZGGm
- The encryption keep going this way until finishing the plain text

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

Classical Encryption Techniques

2. Substitution technique: Polyalphabetic Cipher

- Due to the polyalphabetic nature of the Alberti Cipher (that is, the same plaintext letter is not always encrypted to the same ciphertext letter), it was a very secure cipher when it was invented.

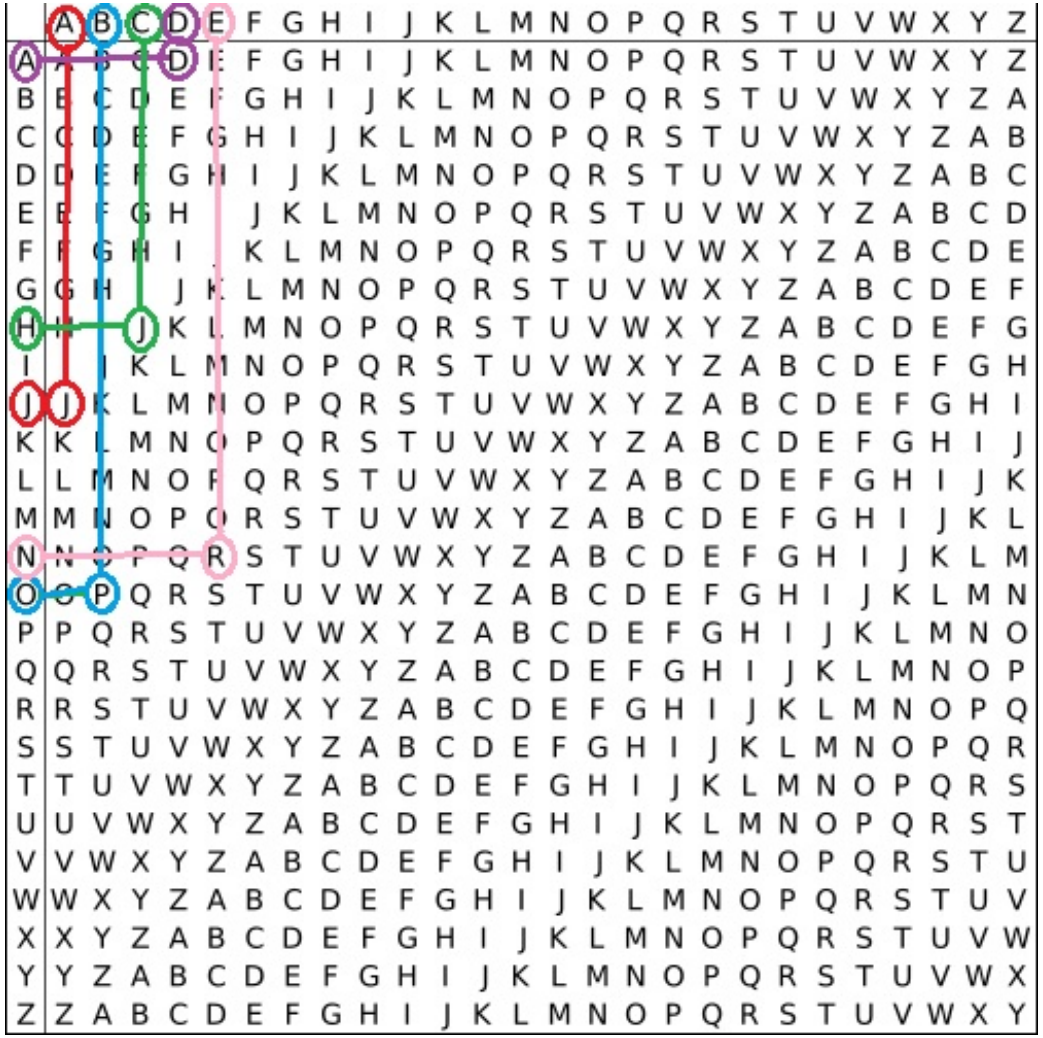
- Another early example of a polyalphabetic cipher was invented by Johannes Trithemius in the 15th Century. Rather than switching alphabets randomly, and indicating it with an uppercase letter, the Trithemius Cipher has the sender change the ciphertext alphabet after each letter was encrypted. This was the first example of a *progressive key cipher*, and he used a tabula recta to show all the different alphabets.

Classical Encryption Techniques

2. Substitution technique: Polyalphabetic Cipher

- Trithemius' idea was to start at the column headed by "A", find the plaintext letter down the far left column, and encrypt this to the ciphertext letter in the first column. You would then move to the next column, and so on.

- For example, the plaintext "johannes trithemius" would be encrypted as follows. The "j" would be found down the left column, and mapped to the letter in the column headed by A (shown in red). This gives "J". The "o" is found down the left column, and traced to the ciphertext in the B column, which is "P" (shown in blue). The "h" (shown in green) gives "J", the "a" (shown in purple) gives "D", and the "n" (shown in pink) gives "R". Continuing in this way we get "JPJDRSKZ BASETRAXKJ".



Classical Encryption Techniques

2. Substitution technique: Playfair Cipher

- The **Playfair cipher** was the first practical digraph substitution cipher. The scheme was invented in **1854** by **Charles Wheatstone** but was named after Lord Playfair who promoted the use of the cipher. In Playfair, cipher unlike *traditional cipher* we encrypt a pair of alphabets (digraphs) instead of a single alphabet.

- It was used for tactical purposes by British forces in the Second Boer War and in World War I and for the same purpose by the Australians during World War II. This was because Playfair is reasonably fast to use and requires no special equipment.

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

Classical Encryption Techniques

2. Substitution technique: Playfair Cipher

- Encryption Techniques:

We can follow 2 main steps with 3 rules to encrypt a plaintext using the Playfair Cipher.

- First, we need to set a key; Exp: monarchy
- Lets the word “instruments” be our plain text to encrypt.

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

✓ Generate the key Square(5×5):The key square is a 5×5 grid of alphabets that acts as the key for encrypting the plaintext. Each of the 25 alphabets must be unique and one letter of the alphabet (usually J) is omitted from the table (as the table can hold only 25 alphabets). If the plaintext contains J, then it is replaced by I.

✓ The initial alphabets in the key square are the unique alphabets of the key in the order in which they appear followed by the remaining letters of the alphabet in order.

Classical Encryption Techniques

2. Substitution technique: Playfair Cipher

- **Algorithm to encrypt the plain text:** The plaintext is split into pairs of two letters (digraphs). If there is an odd number of letters, a Z is added to the last letter.

For example:

```
PlainText: "instruments"
After Split: 'in' 'st' 'ru' 'me' 'nt' 'sz'
```

- **Rules for Encryption:** If both the letters are in the same column: Take the letter below each one (going back to the top if at the bottom).

For example:

```
Diagraph: "me"
Encrypted Text: cl
Encryption: m -> c  e -> l
```

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

Classical Encryption Techniques

2. Substitution technique: Playfair Cipher

- **If both the letters are in the same row**: Take the letter to the right of each one (going back to the leftmost if at the rightmost position).

For example:

```
Diagraph: "st"
Encrypted Text: tl
 Encryption: s -> t t -> l
```

- **If neither of the above rules is true:** Form a rectangle with the two letters and take the letters on the horizontal opposite corner of the rectangle.

For example:

```
Diagraph: "nt"
Encrypted Text: rq
Encryption: n -> r t -> q
```

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

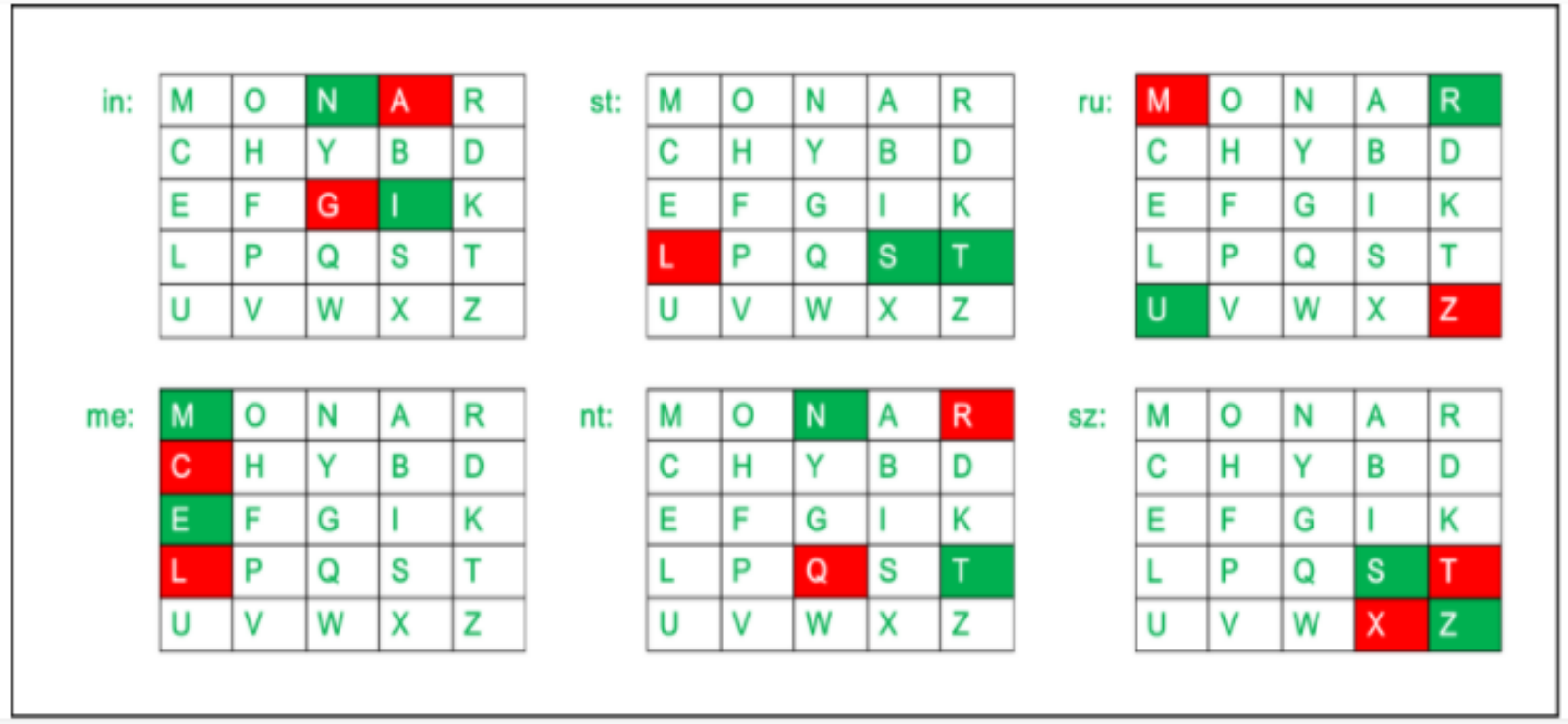
M	O	N	A	R
C	H	Y	B	D
E	F	G	I	K
L	P	Q	S	T
U	V	W	X	Z

Classical Encryption Techniques

2. Substitution technique: Playfair Cipher

Plain Text: "instrumentsz"
Encrypted Text: gatlmzclrqtx
Encryption:

i -> g
n -> a
s -> t
t -> l
r -> m
u -> z
m -> c
e -> l
n -> r
t -> q
s -> t
z -> x



Classical Encryption Techniques

2. Substitution technique: One-Time Pad

- In cryptography, a one-time pad is a system in which a private key generated randomly is used only once to encrypt a message that is then decrypted by the receiver using a matching one-time pad and key.

- Messages encrypted with keys based on randomness have the advantage that there is theoretically no way to "break the code" by analyzing a succession of messages.

- Each encryption is unique and bears no relation to the next encryption so that some pattern can be detected. With a one-time pad.

Classical Encryption Techniques

2. Substitution technique: One-Time Pad

- How it works?
  - ✓ Convert the plaintext to binary.
  - ✓ Generate a key that is totally random. And, in binary, is at least as long as the plaintext or longer.
  - ✓ Produce the ciphertext by applying bitwise XOR on the plaintext and the key.

- Example:
  - Plaintext: Hi! ⟹ 1001000 1101001 0100001
  - Key: 0l;@ ⟹ 0110000 1101100 0111011 1000000 (XOR)
  - Ciphertext ⟹ 1111000 0000101 0011010 1000000

2. Substitution technique: Hill Cipher

- Hill cipher is a polygraphic substitution cipher based on linear algebra. Each letter is represented by a number modulo 26.
- Often the simple scheme A = 0, B = 1, …, Z = 25 is used, but this is not an essential feature of the cipher.
- To encrypt a message, each block of n letters is multiplied by an invertible n × n matrix, against modulus 26.
- To decrypt the message, each block is multiplied by the inverse of the matrix used for encryption.
- The matrix used for encryption is the cipher key, and it should be chosen randomly from the set of invertible n × n matrices (modulo 26)

Classical Encryption Techniques

2. Substitution technique: Hill Cipher: Example

```
Input : Plaintext: ACT
Key: GYBNQKURP
Output : Ciphertext: POH
```

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$$

We have to encrypt the message 'ACT' (n=3).The key is 'GYBNQKURP' which can be written as the nxn matrix:

The message 'ACT' is written as vector:

$$\begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix}$$

The enciphered vector is given as:

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix} \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix} = \begin{bmatrix} 67 \\ 222 \\ 319 \end{bmatrix} \equiv \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix} \pmod{26}$$

which corresponds to ciphertext of 'POH'

2. Substitution technique: Hill Cipher: Example

- To decrypt the message, we turn the ciphertext back into a vector, then simply multiply by the inverse matrix of the key matrix .The inverse of the matrix used in the previous example is:

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}^{-1} \equiv \begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix} \pmod{26}$$

For the previous Ciphertext ‘POH’:

$$\begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix} \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix} \equiv \begin{bmatrix} 260 \\ 574 \\ 539 \end{bmatrix} \equiv \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix} \pmod{26}$$

which gives us back ‘ACT’.

Classical Encryption Techniques

3. Transposition Cipher

- Transposition Cipher is a cryptographic algorithm where the order of alphabets in the plaintext is rearranged to form a cipher text. In this process, the actual plain text alphabets are not included.
- A simple example for a transposition cipher is columnar transposition cipher where each character in the plain text is written horizontally with specified alphabet width. The cipher is written vertically, which creates an entirely different cipher text.
- Consider the plain text hello world, and let us apply the simple columnar transposition technique.
- The plain text characters are placed horizontally and the cipher text is created with vertical format as : **holewdlo lr.** Now, the receiver has to use the same table to decrypt the cipher text to plain text.

h	e	l	l
o	w	o	r
l	d		

Classical Encryption Techniques

3. Transposition Cipher: Book Cipher or Running Key Cipher

- The book cipher or the running key cipher works on the basic principle of one-time pad cipher. In onetime pad cipher the key is taken as long as the plain text and is discarded after the use. Every time a new key is taken for a new message.

- The improvement to the onetime pad in Book cipher is that the key or the onetime pad is taken from the book. Let us discuss the steps:

  - ✓ **Step 1:** Convert the plain text in numeric form consider A=0, B=1, C=3 …, Z=25.
  - ✓ **Step 2:** Take a onetime pad or key from any of the books and convert it in the numeric form also. But the key must be as long as the length of plain text.
  - ✓ **Step 3:** Now add the numeric form of both plain text and key, each plain text letter with corresponding key text letter. If the addition of any plain text letter with corresponding key text letter is >26, then subtract it with 26.

Classical Encryption Techniques

Ubiquitous Computing & Security Laboratory

3. Transposition Cipher: Book Cipher or Running Key Cipher: Example

Let us understand with the example:

- **Plain text:** Meet Tomorrow
- **Key** taken from the book: ANENCRYPTION.
- Now we have to convert this plain text and key text in numeric form and add them to get cipher text as shown in the below:

Numeric form Plian Text	M	E	E	T	T	O	M	O	R	R	O	W	
	12	4	4	19	19	14	12	14	17	17	14	22	
Numeric from Key Text	A	N	E	N	C	R	Y	P	T	I	O	N	
	0	13	4	13	2	17	24	15	19	8	14	13	
Add the numeric form of Plain text and Key Text:													
	12	4	4	19	19	14	12	14	17	17	14	22	
+	0	13	4	13	2	17	24	15	19	8	14	13	
Subtract Numbers > 26 by 26	12	17	8	32	21	31	36	29	36	25	28	35	
	12	17	8	6	21	5	10	3	10	25	3	9	
New Cipher Text	M	R	I	G	V	F	K	D	K	Z	D	J	

3. Product Cipher

- **Product cipher**, data encryption scheme in which the ciphertext produced by encrypting a plaintext document is subjected to further encryption. By combining two or more simple transposition ciphers or substitution ciphers, a more secure encryption may result.

- One of the most famous field ciphers of all time was a fractionation system, the ADFGVX cipher employed by the German army during World War I. This system used a 6 × 6 matrix to substitution-encrypt the 26 letters and 10 digits into pairs of the symbols A, D, F, G, V, and X. The resulting biliteral cipher was then written into a rectangular array and route encrypted by reading the columns in the order indicated by a key word.

- The great French cryptanalyst Georges J. Painvin succeeded in cryptanalyzing critical ADFGVX ciphers in 1918, with devastating effect for the German army in the battle for Paris.

Classical Encryption Techniques

3. Product Cipher: Example

bilateral substitution array

	A	D	F	G	V	X
A	C	O	8	X	F	4
D	M	K	3	A	Z	9
F	N	W	L	0	J	D
G	5	S	I	Y	H	U
V	P	1	V	B	6	R
X	E	Q	7	T	2	G

intermediate ciphertext:

W	E		A	R	E		D	I	S	C	O	V	E	R	E	D
FD	XA		DG	VX	XA		FX	GF	GD	AA	AD	VF	XA	VX	XA	FX

S	A	V	E		Y	O	U	R	S	E	L	F
GD	DG	VF	XA		GG	AD	GX	VX	GD	XA	FF	AV

transposition matrix

A	U	T	H	O	R
1	6	5	2	3	4
F	D	X	A	D	G
V	X	X	A	F	X
G	F	G	D	A	A
A	D	V	F	X	A
V	X	X	A	F	X
G	D	D	G	V	F
X	A	G	G	A	D
G	X	V	X	G	D
X	A	F	F	A	V

ciphertext:

F V G A V	G X G X A	A D F A G	G X F D F
A X F V A	G A G X A	A X F D D	V X X G V
X D G V F	D X F D X	D A X A	

Conclusion

- In this chapter, we reviewed some of the classical encryption techniques, and discussed how they work.
- Those techniques were mainly used manually to encrypt messages during the war.
- A thoughtful Frequency analysis is capable to break the cipher of most of those classical techniques, however, they are the main foundation and pilar to modern cryptography.

Classical Encryption Techniques

THANK YOU!

Presented by

Abir EL.

Abir.el@seoultech.ac.kr