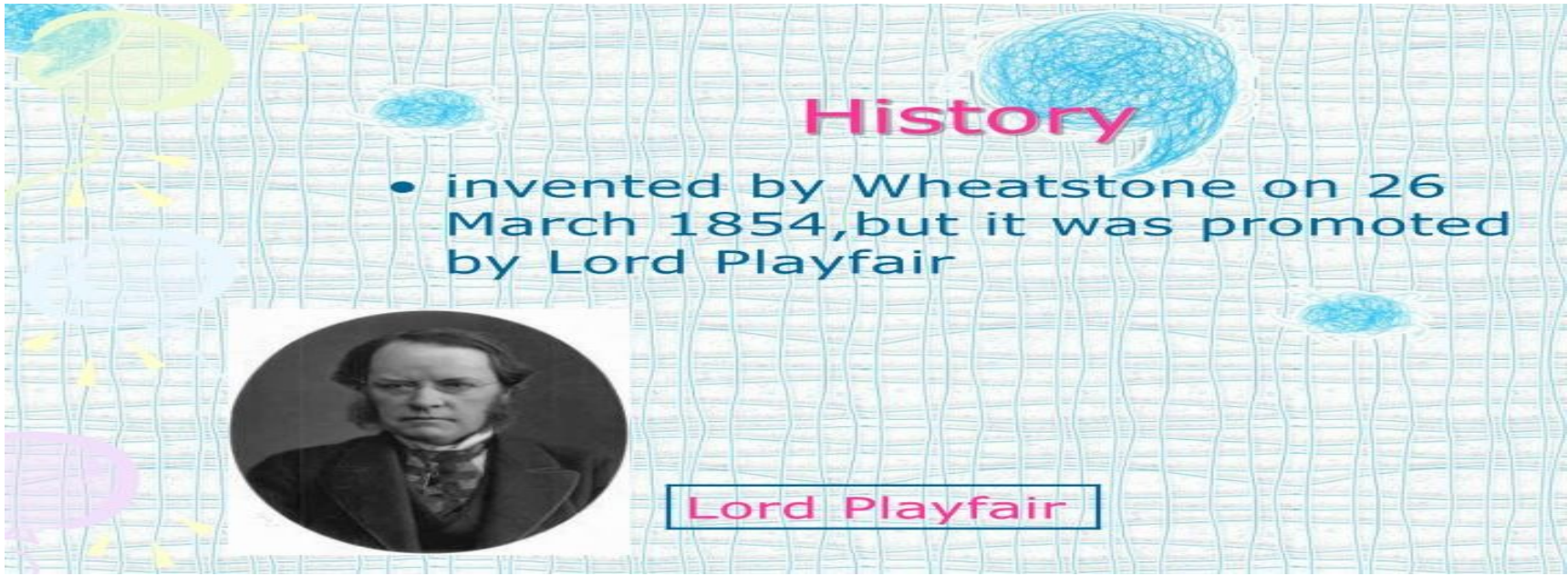
19Z701 - CRYPTOGRAPHY

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 tra ditional cipher we encrypt a pair of alphabets(digraphs) instead of a single alphabet.



- It was rejected by the British Foreign Office when it was developed
- It was used for tactical purposes in the Second Boer and World War I by British
- for the same purpose by the Australians and Germans during World War II

- Playfair is now regarded as insecure for any purpose because modern hand-held computers could easily break the cipher within seconds
- The first published solution of the Playfair cipher was published in 1914

Digraph Substitution Ciphers

- Digraph Substitution Ciphers are similar to Monoalphabetic Substitution Ciphers, except that instead of replacing individual letters in the plaintext, they replace pairs of letters with another pair of letters (or digraph).

Encryption Technique

The Algorithm consists of 2 steps:

1. **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.

2.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.

PlainText: "instruments"

After Split: 'in' 'st' 'ru' 'me' 'nt' 'sz'

Pair cannot be made with same letter. Break the letter in single and add a bogus letter to the previous letter.

Plain Text: “hello”
After Split: ‘he’ ‘lx’ ‘lo’
Here **‘x’** is the bogus letter.

If the letter is standing alone in the process of pairing, then add an extra bogus letter with the alone letter

Plain Text: “helloe”
AfterSplit: ‘he’ ‘lx’ ‘lo’ ‘ez’
Here **‘z’** is the bogus letter.

plaintext is encrypted two letters at a time

1. if a pair is a repeated letter, insert filler like 'X’
2. if both letters fall in the same row, replace each with letter to right (wrapping back to start from end)
3. if both letters fall in the same column, replace each with the letter below it (again wrapping to top from bottom)
4. otherwise each letter is replaced by the letter in the same row and in the column of the other letter of the pair

plaintext encrypted two letters at a time:

1.if a pair is a repeated letter, insert a filler like 'X', eg. "balloon" encrypts as "ba lx lo on"

2.if both letters fall in the same row, replace each with letter to right (wrapping back to start from end), eg. “ar" encrypts as "RM"

3.if both letters fall in the same column, replace each with the letter below it (again wrapping to top from bottom), eg. “mu" encrypts to "CM"

4.otherwise each letter is replaced by the one in its row in the column of the other letter of the pair, eg. “hs" encrypts to "BP", and “ea" to "IM" or "JM" (as desired)

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

5X5 matrix of letters

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

- **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

For example:

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

❖ **Substitution Cipher Types**

2. Polyalphabetic Cipher Types

D. Playfair Cipher

- **Example1: Plaintext:** CRYPTO IS TOO EASY **Key =** INFOSEC **Ciphertext:** ??

Grouped text: CR YP TO IS TO XO EA SY

Ciphertext: AQ TV YB NI YB YF CB OZ

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

❖ **Substitution Cipher Types**

2. Polyalphabetic Cipher Types

D. Playfair Cipher

- **Example2: Ciphertext:** AQTVYBNIYBYFCBOZ **Key =** INFOSEC **Plaintext:** ??

Grouped text: AQ TV YB NI YB YF CB OZ

Plaintext: CR YP TO IS TO XO EA SY

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

- **To Decrypt:** The receiver reconstructs the 5 x 5 matrix using the keyword and then uses the same rules as for encryption.

Thank You