# Week 2 Practical: *Hill cipher & Playfair cipher*

Dr. Qublai Ali K. Mirza and Madhu Khuruna

University of Gloucestershire

qamirza@glos.ac.uk

UNIVERSITY OF GLOUCESTERSHIRE

# Overview

# Alphabet index

| A | B | C | D | E | F | G | H | I | J | K | L | M |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |
| . | _ | ? | | | | | | | | | | |
| 26 | 27 | 28 | | | | | | | | | | |

Table: Alphabet and their indices

# Recap

- Last week, we established that classical ciphers can be classified into
  - Substitution ciphers
  - Polygraphic ciphers
- We looked at Caesar and Vigenère ciphers as examples of *substitution* ciphers
- This week we will look at *Hill cipher* and *Fairplay cipher*

# Overview

- Created by Lester S. Hill in 1929
- Polygraphic Substitution Cipher
- Uses matrices to encrypt and decrypt
- Uses modular arithmetic (Mod 26)

# Modular arithmetic recap

- Given two numbers *a* and *b*, a modular operation takes the *remainder/modulo* of a division operation on *a* by *b*
- Denoted by mod

$$r = a \bmod b$$

- For example,
  - $0 \bmod 26 = 0$
  - $10 \bmod 26 = 10$
  - $27 \bmod 26 = 1$
  - $30 \bmod 26 = 4$

# How it works

- One matrix to encrypt, one to decrypt
- Must be $n \times n$, invertible matrices
- Decryption matrix must be modular inverse of encryption matrix in mod 26

# Example

Suppose that we have a key matrix $K$

$$K = \begin{matrix} 2 & 1 \\ 3 & 4 \end{matrix}$$

to encrypt *plaintext* $P = CRYPTO$

# Example

Step 1: Organise plaintext into a matrix

$$P = \begin{matrix} C & Y & T \\ R & P & O \end{matrix}$$

Step 2: Convert each character into their corresponding indices

$$P = \begin{matrix} 2 & 24 & 19 \\ 17 & 15 & 14 \end{matrix}$$

# Example

Step 3: Multiply with key matrix $K$ to get ciphertext $C$:

$$C = K \times P = \begin{matrix} 4+17 & 48+15 & 38+14 \\ 6+68 & 72+60 & 57+56 \end{matrix} \quad mod\ 26$$

$$= \begin{matrix} 21 & 63 & 52 \\ 74 & 132 & 113 \end{matrix} \quad mod\ 26$$

$$= \begin{matrix} 21 & 11 & 0 \\ 22 & 2 & 9 \end{matrix} = \begin{matrix} V & L & A \\ W & C & J \end{matrix} = VWLCAJ$$

# Decryption

- Now that we have got our ciphertext $C$ together with key $K$, decrypting it is pretty straightforward
- It is done by using this equation

$$P = (K^{-1} \times C) \bmod 26$$

- But first we have to get the *inverse* of $K$ (i.e., $K^{-1}$), using what we discussed in the lecture slides
- But we need to get two things first:
  - Determinant of $K$ det(K)
  - *modulo inverse* $M$ of det(K)

# Modulo inverse

- The modulo inverse $M$ of an integer $A$ is an integer $A^{-1}$ such that

$$AA^{-1} \ mod \ m = 1$$

- So for instance the modulo inverse of 9 with respect to 26 would be 3, since

$$(9 \times 3) \ mod \ 26 = 1$$

# Example: Decryption

Given the key matrix $K$

$$K = \begin{matrix} 2 & 1 \\ 3 & 4 \end{matrix}$$

Step 1: Get the determinant $det(K)$

$$M = det(K) = 2 \times 4 - 3 \times 1 = 5$$

Step 2: Get the modulo inverse $M^{-1}$ of M with respect to 26, which would be 21 since

$$(5 \times 21) \; mod \; 26 = 1$$

# Example:Decryption

Step 3: Get the inverse matrix $K^{-1}$ of $K$ using

$$K^{-1} = M^{-1} \begin{matrix} 4 & -1 \\ -3 & 2 \end{matrix} \ mod\ 26$$

$$= 21 \begin{matrix} 4 & -1 \\ -3 & 2 \end{matrix} \ mod\ 26$$

$$= \begin{matrix} 4 \times 21 & -1 \times 21 \\ -3 \times 21 & 2 \times 21 \end{matrix} \ mod\ 26 = \begin{matrix} 6 & 5 \\ 15 & 16 \end{matrix}$$

# Example: Decryption

Step 3: With ciphertext

$$C = VWLCAJ = \begin{matrix} V. & L & A \\ W. & C & J \end{matrix} = \begin{matrix} 21 & 11 & 0 \\ 22 & 2 & 9 \end{matrix}$$

Getting plaintext $P$ then becomes

$$P = K^{-1} \times C = \begin{matrix} 6 & 5 \\ 15 & 16 \end{matrix} \times \begin{matrix} 21 & 11 & 0 \\ 22 & 2 & 9 \end{matrix} \bmod 26 = CRYPTO$$

# Hill Cipher on CryptTool 2

- From the *CryptTool 2* startup menu, click *Cryptography*
- Then click *Classical* and then select *Hill cipher*
- In the plaintext section of *TextInput*, type in: *roses are red*
- Then in the *Hill cipher* box, type in:

$$\begin{matrix} 2 & 1 \\ 3 & 4 \end{matrix}$$

- Finally click on the *Play* button to execute

# Hill Cipher on CryptTool 2


Figure: Hill Cipher on CryptTool 2

# Overview

- Invented by Charles Wheatstone in 1854
- Encrypts *two* letters at a time
- Features a 5 × 5 matrix of letters based on a keyword
- Fill in letters of keyword (sans duplicates)
- Fill rest of matrix with other letters

# Rules of the Playfair cipher

1. If a pair is a repeated letter, insert a filler like "X". E.g., "hallway" would become ha lx wa yx
2. If both letters fall in the same row, replace each with letter to right.
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 one in its row in the column of the other letter of the pair

# Example

Given the keyword $K$ ="HELLO" and plaintext $P$ ="CRYPTO",
Step 1: Arrange $K$ into a $5 \times 5$ matrix, making it like so:

$$\begin{matrix} H & E & L & O & A \\ B & C & D & F & G \\ I & K & M & N & P \\ Q & R & S & T & U \\ V & W & X & Y & Z \end{matrix}$$

Step 2: Break down $P$ into two letter pairs, like so: CR YP TO

# Example (cont.)

Step 3: Encrypt each pair using the 4 rules and the key matrix, so

$$\begin{aligned} \text{CR} &\longrightarrow KW \\ \text{YP} &\longrightarrow ZN \\ \text{TO} &\longrightarrow YF \end{aligned}$$

Step 4: The encrypted ciphertext $C$ then becomes: $KWZNYF$

# Playfair Cipher on CryptTool 2

- From the *CryptTool 2* startup menu, click *Cryptography*
- Then click *Classical* and then select *Playfair cipher*
- In the plaintext section of *TextInput*, type in: *CRYPTO*
- Next double-click on the *Playfair cipher* box to open up its settings
- Then type in *HELLO* in the Key Value
- Finally minimize it and click on the *Play* button to execute

# Playfair Cipher on CryptTool 2

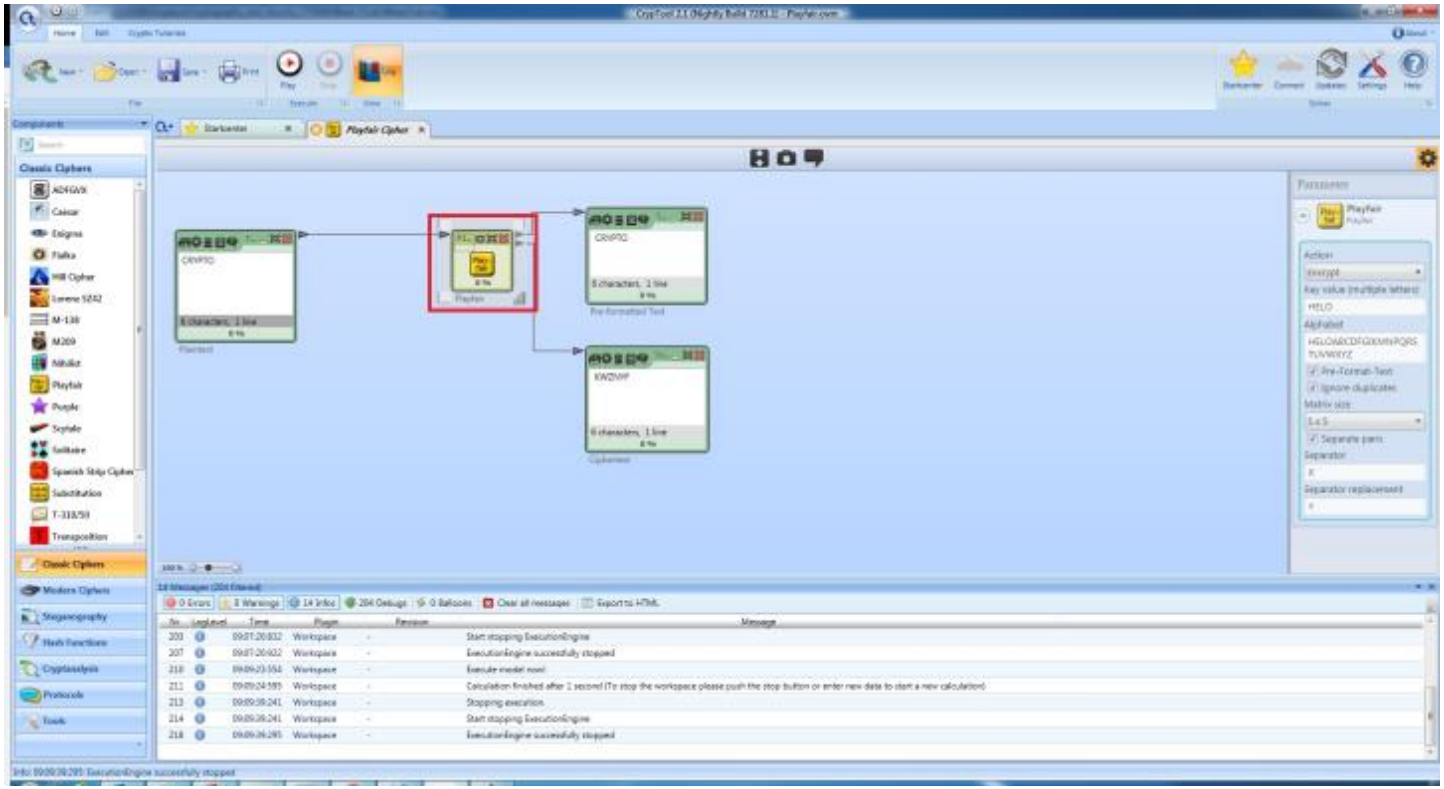

Figure: Playfair Cipher on CryptTool 2

# Playfair Cipher on CryptTool 2

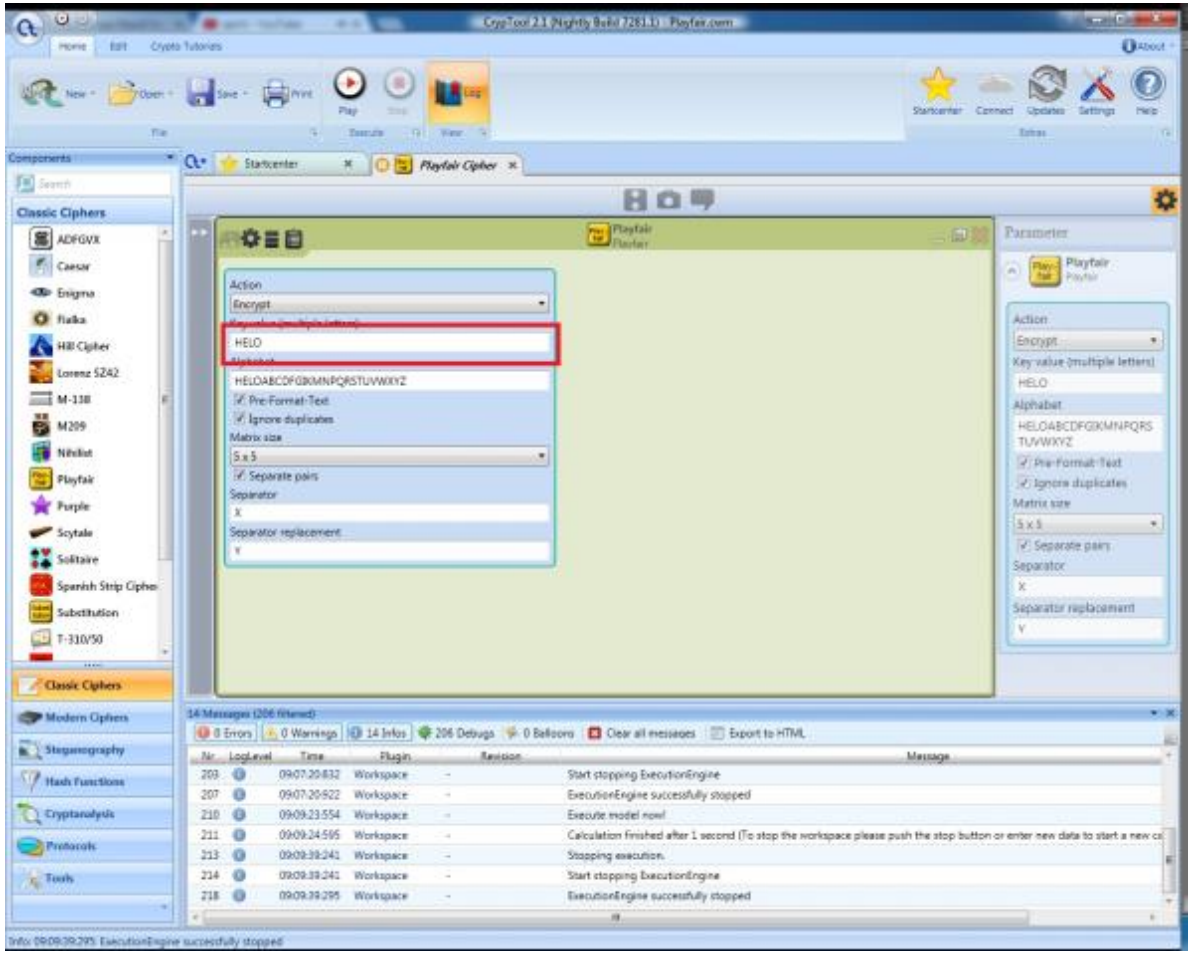


Figure: Playfair Cipher key configuration

# Bringing it all together

- We looked at both *Hill* and *Playfair* ciphers
- We also looked at how each of them works and how to get them working in *CrypTool 2*
- Next week: *Information theory and classical ciphers*

# Post-sessional work

- Create a CryptTool project which accepts a plaintext, and
  - First encrypts it using *Hill* Cipher
  - Then encrypts the Hill Cipher with Playfair Cipher
  - Then gets the original plaintext back to its original form

# Q & A