3. Polygraphic Ciphers

- Instead of substituting one letter for another letter, a polygraphic cipher performs substitutions with two or more groups of letters.
- This has the advantage of masking the frequency distribution of letters, which makes frequency analysis attackes much more difficult.
- **Playfair Cipher:-** You create 5x5 matrix based on a keyword with the reset of the alphabets characters. For example a keyword (without repetition) such as "PROBLEMS":

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

- In this cipher, we will encipher letters pairs at a time. Consider the following plaintext:

SHE WENT TO THE STORE

- When we pair up the letters they get grouped as follows:

SH EW EN TT OT HE ST OR E

- But, we are not allowed to encipher any double letters. So, in this case, we will insert an Q into the plaintext. (If Q is a double letter, then insert another infrequent letter, say X.)

SH EW EN TQ TO TH ES TO RE

- To encipher pairs of letters, adhere to the following rules:
  - If the two letters are on the same row of the chart, like "ES", then replace each letter by the letter to the right. (If necessary, wrap around to the left end of the row. So "ES" encrypts to "MA".

2. If the two letters are on the same column of the chart, like, "TH", then replace each letter by the letter below it. (If necessary, wrap around to the top end of the column.) So "TH" encrypts to "YT".

3. If two letters are on a different row and column, like, "SH", then replace each letter by another letter on its same row, but in the column of the other letter. So "SH" encrypts to "AG".

- Using these rules, here is the encryption of the plaintext above:

Plaintext : SH EW EN TQ TO TH ES TO RE

Ciphertext: AG MV MK UT QB YT MA QB PM

- To decipher, ignore rule 1. In rules 2 and 3 shift up and left instead of down and right. Rule 4 remains the same. Once you are done, drop any extra Xs that don't make sense in the final message and locate any missing Qs or any Is that should be Js.

Hill Cipher: - The Hill Cipher uses matrix multiplication to encrypt a message.

First, you need to assign two numbers to each letter in the alphabet and also assign numbers to space, . , and ? or !.

The key space is the set of all invertible matrices over Z_{26}. 26 was chosen because there are 26 characters, which solves some problems later on.

$$K = \begin{bmatrix} k_{11} & k_{12} & \dots & k_{1m} \\ k_{21} & k_{22} & \dots & k_{2m} \\ \vdots & \vdots & & \vdots \\ k_{m1} & k_{m2} & \dots & k_{mm} \end{bmatrix}$$

$$C_1 = P_1 k_{11} + P_2 k_{21} + \cdots + P_m k_{m1}$$
$$C_2 = P_1 k_{12} + P_2 k_{22} + \cdots + P_m k_{m2}$$
$$\dots$$
$$C_m = P_1 k_{1m} + P_2 k_{2m} + \cdots + P_m k_{mm}$$

The key matrix in the Hill cipher needs to have a multiplicative inverse as shown :

For example, the plaintext “code is ready” can make a 3 × 4 matrix when adding extra bogus character “z” to the last block and removing the spaces.

For example, the plaintext "code is ready" can make a 3 × 4 matrix when adding extra bogus character "z" to the last block and removing the spaces.

$$\begin{bmatrix} & & & \\ & & & \\ & & & \end{bmatrix}_{C} = \begin{bmatrix} & & & \\ & & & \\ & & & \end{bmatrix}_{P} \begin{bmatrix} & & & \\ & & & \\ & & & \\ & & & \end{bmatrix}_{K}$$

$$\begin{bmatrix} 14 & 07 & 10 & 13 \\ 08 & 07 & 06 & 11 \\ 11 & 08 & 18 & 18 \end{bmatrix} = \begin{bmatrix} 02 & 14 & 03 & 04 \\ 08 & 18 & 17 & 04 \\ 00 & 03 & 24 & 25 \end{bmatrix} \begin{bmatrix} 09 & 07 & 11 & 13 \\ 04 & 07 & 05 & 06 \\ 02 & 21 & 14 & 09 \\ 03 & 23 & 21 & 08 \end{bmatrix}$$

a. Encryption

$$\begin{bmatrix} & & & \\ & & & \\ & & & \end{bmatrix}_{P} = \begin{bmatrix} & & & \\ & & & \\ & & & \end{bmatrix}_{C} \begin{bmatrix} & & & \\ & & & \\ & & & \\ & & & \end{bmatrix}_{K^{-1}}$$

$$\begin{bmatrix} 02 & 14 & 03 & 04 \\ 08 & 18 & 17 & 04 \\ 00 & 03 & 24 & 25 \end{bmatrix} = \begin{bmatrix} 14 & 07 & 10 & 13 \\ 08 & 07 & 06 & 11 \\ 11 & 08 & 18 & 18 \end{bmatrix} \begin{bmatrix} 02 & 15 & 22 & 03 \\ 15 & 00 & 19 & 03 \\ 09 & 09 & 03 & 11 \\ 17 & 00 & 04 & 07 \end{bmatrix}$$

b. Decryption

S".

One-Time Pad: - One of the goals of cryptography is perfect secrecy. A study by Shannon has shown that perfect secrecy can be achieved if each plaintext symbol is encrypted with a key randomly chosen from a key domain. This idea is used in a cipher called one-time pad, invented by **Vernam.**

Example:- Plaintext VERNAMCIPHER

Key 76 48 16 82 44 3 58 11 60 5 48 88

Encryption

Plaintext	21	4	17	13	0	12	2	8	15	7	4	17
												+
Key	76	48	16	82	44	3	58	11	60	5	48	88

Ciphertext	97	52	33	95	44	15	60	19	75	12	52	105
												mod 26
	19	0	7	17	18	15	8	19	23	12	0	1
	t	a	h	r	s	p	i	t	x	m	a	b

Decryption ⊡

Ciphertext	t	a	h	r	s	p	i	t	x	m	a	b	
	19	0	7	17	18	15	8	19	23	12	0	1	
													-
Key	76	48	16	82	44	3	58	11	60	5	48	88	
	---	---	---	---	---	---	---	---	---	---	---	---	---
plaintext	-57	-48	-9	-65	-26	12	-50	8	-37	7	-48	-87	mod 26
	21	4	17	13	0	12	2	8	15	7	4	17	
	V	E	R	N	A	M	C	I	P	H	E	R	