Assignment Number: 2

Name: Divya Shah; Branch: I.T (T.E.); Roll Number: 115 24/08/2023

Aim: Cryptanalysis or decoding of polyalphabetic ciphers: Playfair, Vigenère cipher.

LO mapped: LO1

Theory:

Polyalphabetic ciphers:

Polyalphabetic ciphers have a rich history in the field of cryptography. They offer enhanced security compared to simple substitution ciphers by employing multiple sets of substitutions. This assignment focuses on cryptanalysis, the process of breaking codes, to understand the inner workings of the Playfair and Vigenère ciphers and the methods to crack them.

- Playfair Cipher

The Playfair cipher involves setting up a key table, typically a 5x5 matrix, using a keyword. The key table is used for encryption. To encrypt a message, each pair of letters in the plaintext is substituted based on their positions in the key table. The decryption process follows a similar approach using the inverse of the key table setup.

Playfair Cipher Example:

Plaintext: CRYPTOLOGY

Keyword: KEYWORD

Key Table Setup:

$$K\ E\ Y\ W\ O$$

$$R\ D\ A\ B\ C$$

$$F\ G\ H\ I\ L$$

$$M\ N\ P\ Q\ S$$

$$T\ U\ V\ X\ Z$$

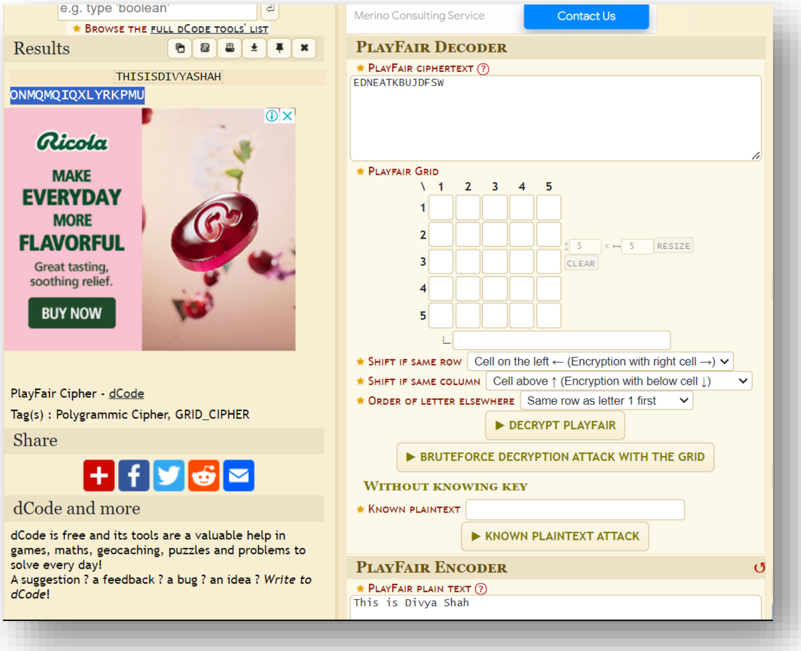
Encryption:

i. Divide the plaintext into pairs: CR YP TO LO GY
ii. Find each pair in the key table and apply the encryption rule.
iii. Resulting Ciphertext: GA CI XN HP IQ

Decryption:

i. Reverse the process using the decryption formula.

ii. Original Plaintext: CR YP TO LO GY


e.g. type 'boolean'
Browse the full dCode tools' list
Merino Consulting Service
Contact Us

Results

THISISDIVYASHAH

ONMQMQIQXLYRKPMU

Ricola
MAKE EVERYDAY MORE FLAVORFUL
Great tasting, soothing relief.
BUY NOW

PlayFair Cipher - dCode

Tag(s) : Polygrammic Cipher, GRID_CIPHER

Share

dCode and more

dCode is free and its tools are a valuable help in games, maths, geocaching, puzzles and problems to solve every day!
A suggestion ? a feedback ? a bug ? an idea ? *Write to dCode!*

PlayFair Decoder

★ PlayFair ciphertext

EDNEATKBUJDFSW

★ Playfair Grid

\	1	2	3	4	5
1					
2					
3					
4					
5					

5 × 5 RESIZE CLEAR

★ Shift if same row: Cell on the left ← (Encryption with right cell →)

★ Shift if same column: Cell above ↑ (Encryption with below cell ↓)

★ Order of letter elsewhere: Same row as letter 1 first

▶ DECRYPT PLAYFAIR

▶ BRUTEFORCE DECRYPTION ATTACK WITH THE GRID

Without knowing key

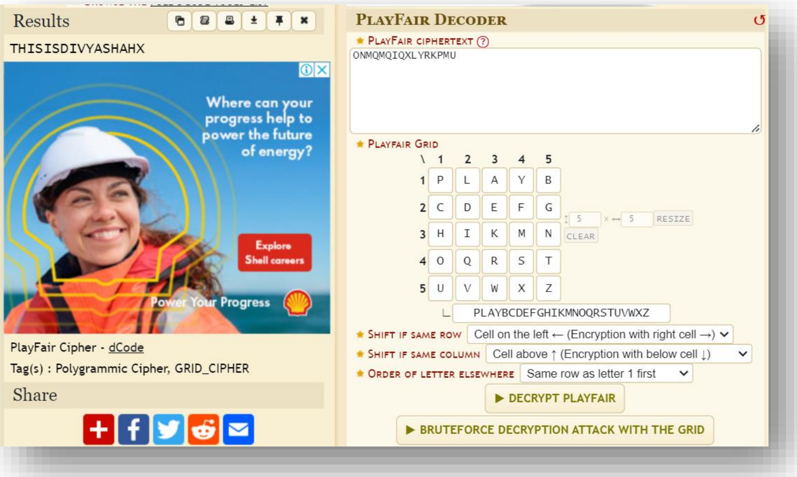
★ Known plaintext

▶ KNOWN PLAINTEXT ATTACK

PlayFair Encoder

★ PlayFair plain text

This is Divya Shah



Results

THISISDIVYASHAHX

PlayFair Cipher - dCode

Tag(s) : Polygrammic Cipher, GRID_CIPHER

Share

PlayFair Decoder

★ PlayFair ciphertext

ONMQMQIQXLYRKPMU

★ Playfair Grid

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

PLAYBCDEFGHIKMNOQRSTUVWXZ

5 × 5 RESIZE CLEAR

★ Shift if same row: Cell on the left ← (Encryption with right cell →)

★ Shift if same column: Cell above ↑ (Encryption with below cell ↓)

★ Order of letter elsewhere: Same row as letter 1 first

▶ DECRYPT PLAYFAIR

▶ BRUTEFORCE DECRYPTION ATTACK WITH THE GRID

- Vigenère Cipher

The Vigenère cipher employs a keyword that is repeated to match the length of the plaintext. The key letters are then used to shift the plaintext letters to generate the ciphertext. Decryption involves reversing the process using the same keyword and shifting in the opposite direction.

Vigenère Cipher Example:

Plaintext: CRYPTOLOGY

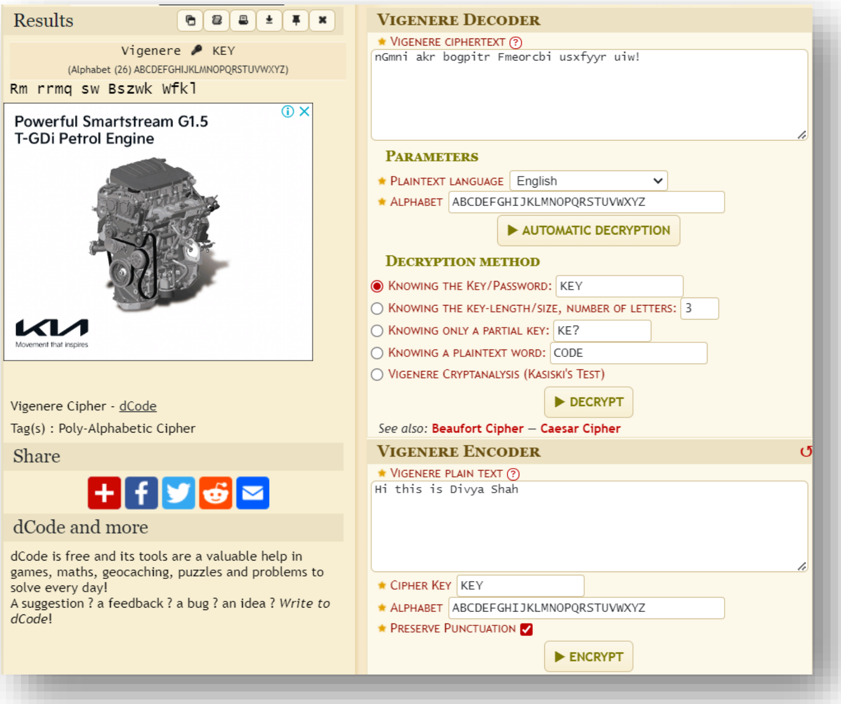
Keyword: CODE

Encryption:

1. Repeat the keyword to match the plaintext length: CODECODECO
2. Shift each letter in the plaintext by the corresponding keyword letter.
3. Resulting Ciphertext: GIDAKWFTQW

Decryption:

1. Reverse the process using the decryption formula.
2. Original Plaintext: CRYPTOLOGY



Results

Vigenere 🔑 KEY
(Alphabet (26) ABCDEFGHIJKLMNOPQRSTUVWXYZ)

```
Rm rrmq sw Bszwk Wfkl
```

Vigenere Cipher - dCode

Tag(s) : Poly-Alphabetic Cipher

Share

dCode and more

dCode is free and its tools are a valuable help in games, maths, geocaching, puzzles and problems to solve every day!
A suggestion ? a feedback ? a bug ? an idea ? *Write to dCode*!

VIGENERE DECODER

★ VIGENERE CIPHERTEXT

```
nGmni akr bogpitr Fmeorcbi usxfyyr uiw!
```

PARAMETERS

★ PLAINTEXT LANGUAGE: English
★ ALPHABET: ABCDEFGHIJKLMNOPQRSTUVWXYZ

▶ AUTOMATIC DECRYPTION

DECRYPTION METHOD

● KNOWING THE KEY/PASSWORD: KEY
○ KNOWING THE KEY-LENGTH/SIZE, NUMBER OF LETTERS: 3
○ KNOWING ONLY A PARTIAL KEY: KE?
○ KNOWING A PLAINTEXT WORD: CODE
○ VIGENERE CRYPTANALYSIS (KASISKI'S TEST)

▶ DECRYPT

See also: Beaufort Cipher – Caesar Cipher

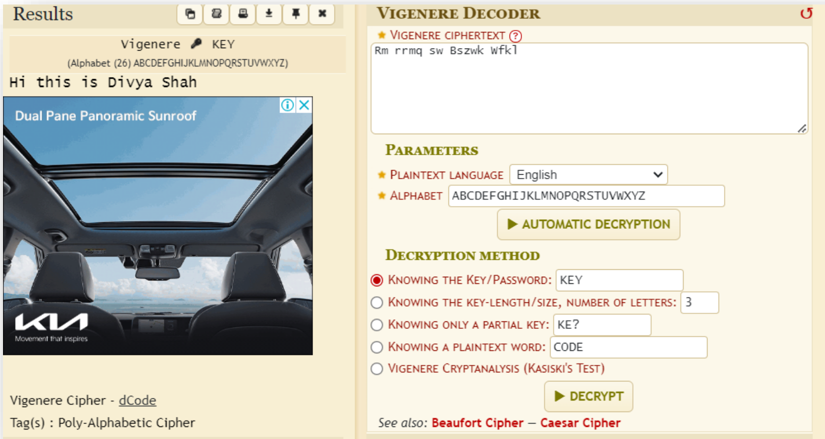
VIGENERE ENCODER

★ VIGENERE PLAIN TEXT

```
Hi this is Divya Shah
```

★ CIPHER KEY: KEY
★ ALPHABET: ABCDEFGHIJKLMNOPQRSTUVWXYZ
★ PRESERVE PUNCTUATION ☑

▶ ENCRYPT



Results

Vigenere 🔑 KEY
(Alphabet (26) ABCDEFGHIJKLMNOPQRSTUVWXYZ)

```
Hi this is Divya Shah
```

Vigenere Cipher - dCode

Tag(s) : Poly-Alphabetic Cipher

VIGENERE DECODER

★ VIGENERE CIPHERTEXT

```
Rm rrmq sw Bszwk Wfkl
```

PARAMETERS

★ PLAINTEXT LANGUAGE: English
★ ALPHABET: ABCDEFGHIJKLMNOPQRSTUVWXYZ

▶ AUTOMATIC DECRYPTION

DECRYPTION METHOD

● KNOWING THE KEY/PASSWORD: KEY
○ KNOWING THE KEY-LENGTH/SIZE, NUMBER OF LETTERS: 3
○ KNOWING ONLY A PARTIAL KEY: KE?
○ KNOWING A PLAINTEXT WORD: CODE
○ VIGENERE CRYPTANALYSIS (KASISKI'S TEST)

▶ DECRYPT

See also: Beaufort Cipher – Caesar Cipher

Conclusion: This assignment has provided a hands-on opportunity to explore and dissect the Playfair and Vigenère ciphers. Through the examples and decryption exercises, you have gained insights into the strengths and vulnerabilities of these historical encryption techniques. As cryptography continues to evolve, understanding these foundational ciphers becomes essential to appreciating the advancements in modern encryption methods.