Security Lab T22
79. Khalid Qureshi

Aim:

Cryptanalysis or decoding of polyalphabetic ciphers: Playfair, Vigenere cipher.

LO Mapping: LO1

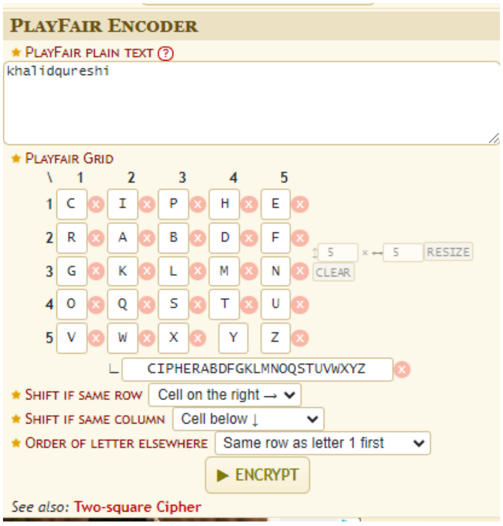
Theory & Output:

Playfair Cipher

The Playfair cipher is a manual symmetric encryption technique and was the first digraph substitution cipher. The scheme was invented in 1854 by Charles Wheatstone, but it was named after Lord Playfair who promoted its use. It encrypts pairs of letters (digraphs) instead of single letters, which makes it significantly harder to break than simpler substitution ciphers.

Key Features:

1. **Key Square:**
    - The Playfair cipher uses a 5x5 grid filled with letters of the alphabet. Normally, the letters "I" and "J" are combined, so the 26-letter alphabet fits into the 25 spaces of the square.
    - The key square is filled with a keyword first, omitting any duplicate letters, and then the remaining letters of the alphabet.
2. **Encryption Process:**
    - The plaintext message is split into pairs of letters. If there are any repeated letters in a pair or if there's a single remaining letter, an 'X' is added to adjust.
    - Each pair of letters is encrypted according to their position in the key square:
        - If both letters are in the same row, each letter is replaced with the letter immediately to its right (wrapping around to the beginning of the row if necessary).
        - If both letters are in the same column, each letter is replaced with the letter immediately below it (wrapping around to the top of the column if necessary).
        - If the letters form a rectangle, each letter is replaced by the letter on the same row but at the column of the other letter in the pair.



PLAYFAIR ENCODER

★ PLAYFAIR PLAIN TEXT

```
khalidqureshi
```

★ PLAYFAIR GRID

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

5 × 5 RESIZE CLEAR

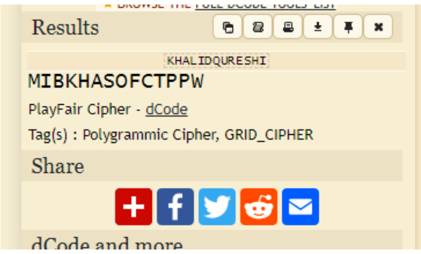
CIPHERABDFGKLMNOQSTUVWXYZ

★ SHIFT IF SAME ROW: Cell on the right →

★ SHIFT IF SAME COLUMN: Cell below ↓

★ ORDER OF LETTER ELSEWHERE: Same row as letter 1 first

See also: Two-square Cipher



Results

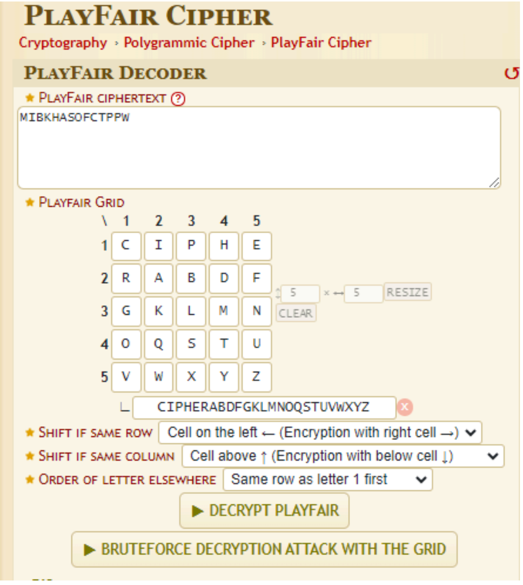
KHALIDQURESHI

```
MIBKHASOFCTPPW
```

PlayFair Cipher - dCode

Tag(s) : Polygrammic Cipher, GRID_CIPHER

3. **Decryption Process:**
   - Decryption is the reverse of encryption:
     - If both letters are in the same row, each letter is replaced with the letter immediately to its left.
     - If both letters are in the same column, each letter is replaced with the letter immediately above.
     - If the letters form a rectangle, each letter is replaced by the letter on the same row but at the column of the other letter in the pair.

- 

PLAYFAIR CIPHER

Cryptography › Polygrammic Cipher › PlayFair Cipher

PLAYFAIR DECODER

★ PLAYFAIR CIPHERTEXT

```
MIBKHASOFCTPPW
```

★ PLAYFAIR GRID

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

5 × 5 RESIZE CLEAR

CIPHERABDFGKLMNOQSTUVWXYZ

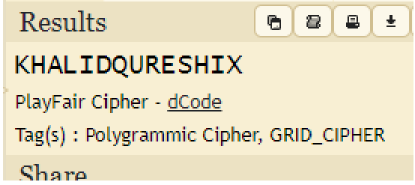
★ SHIFT IF SAME ROW: Cell on the left ← (Encryption with right cell →)

★ 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



Results

KHALIDQURESHIX

PlayFair Cipher - dCode

Tag(s) : Polygrammic Cipher, GRID_CIPHER

Share

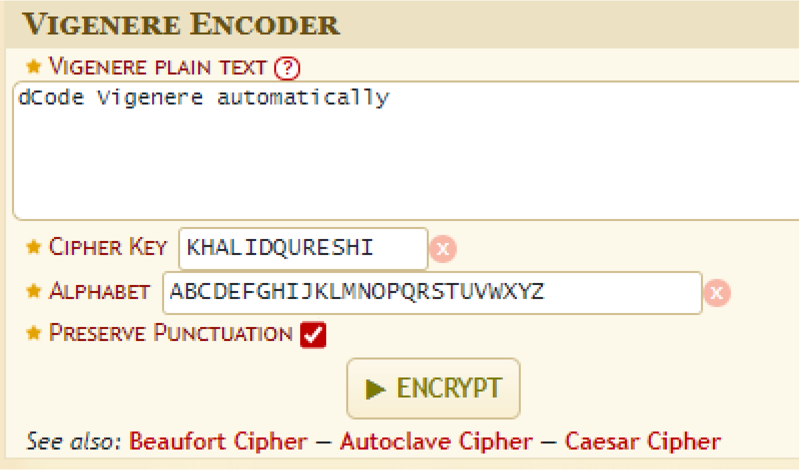
Vigenère Cipher

The Vigenère cipher is a method of encrypting alphabetic text by using a simple form of polyalphabetic substitution. A keyword is repeated until it matches the length of the plaintext. Each letter of the plaintext is then shifted along some number of places defined by the corresponding letter of the key.

Key Features:

1. **Key:**
   - The Vigenère cipher uses a keyword, where each letter of the keyword specifies a shift for the corresponding letter of the plaintext.
2. **Encryption Process:**
   - The plaintext is written out, and the keyword is repeated until it matches the length of the plaintext.
   - Each letter of the plaintext is shifted along the alphabet by the number of positions defined by the corresponding letter of the keyword (where A = 0, B = 1, ..., Z = 25).
   - For example, with keyword "LEMON" and plaintext "ATTACKATDAWN":
     - A + L = L
     - T + E = X
     - T + M = F
     - A + O = O
     - C + N = P

- K + L = V
- And so on.



VIGENERE ENCODER

★ VIGENERE PLAIN TEXT ?

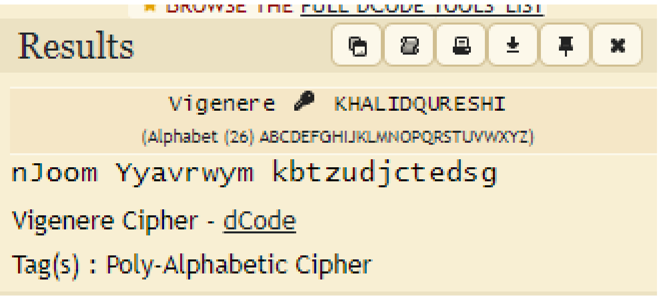
```
dCode Vigenere automatically
```

★ CIPHER KEY: KHALIDQURESHI

★ ALPHABET: ABCDEFGHIJKLMNOPQRSTUVWXYZ

★ PRESERVE PUNCTUATION ☑

See also: Beaufort Cipher – Autoclave Cipher – Caesar Cipher



★ BROWSE THE FULL DCODE TOOLS LIST

Results

Vigenere 🔑 KHALIDQURESHI

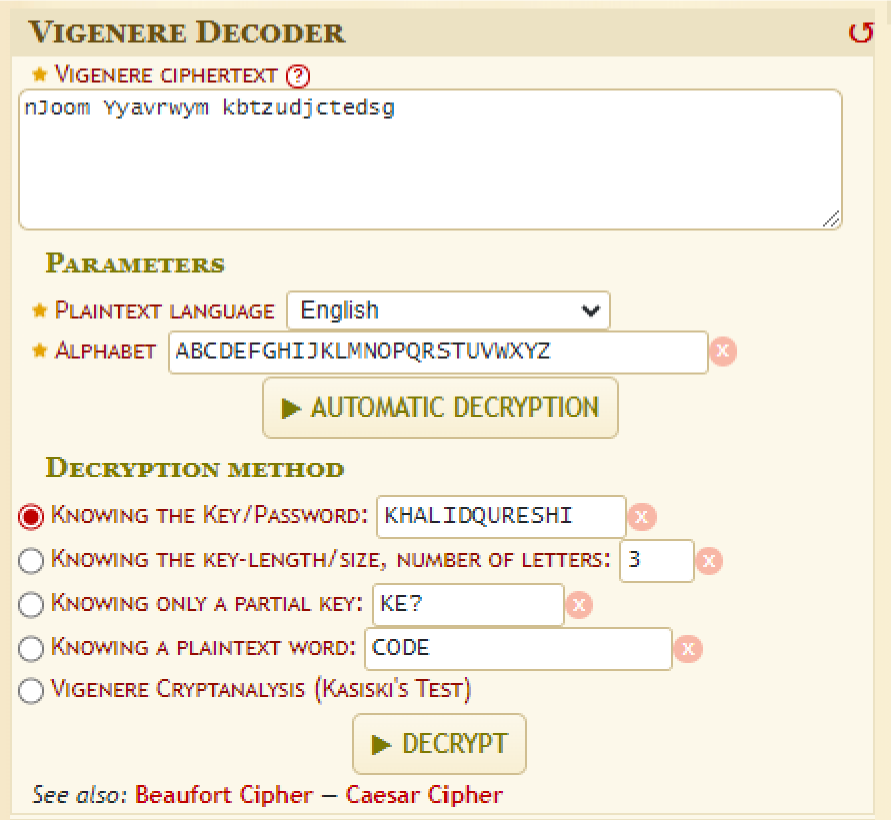
(Alphabet (26) ABCDEFGHIJKLMNOPQRSTUVWXYZ)

```
nJoom Yyavrwym kbtzudjctedsg
```

Vigenere Cipher - dCode

Tag(s) : Poly-Alphabetic Cipher

3. **Decryption Process:**
   - The ciphertext is written out, and the keyword is repeated until it matches the length of the ciphertext.
   - Each letter of the ciphertext is shifted backwards by the number of positions defined by the corresponding letter of the keyword.
   - For example, with keyword "LEMON" and ciphertext "LXFOPVEFRNHR":
     - L - L = A
     - X - E = T
     - F - M = T
     - O - O = A
     - P - N = C
     - V - L = K
     - And so on.



★ Vigenere ciphertext

```
nJoom Yyavrwym kbtzudjctedsg
```

★ Plaintext language: English

★ Alphabet: ABCDEFGHIJKLMNOPQRSTUVWXYZ

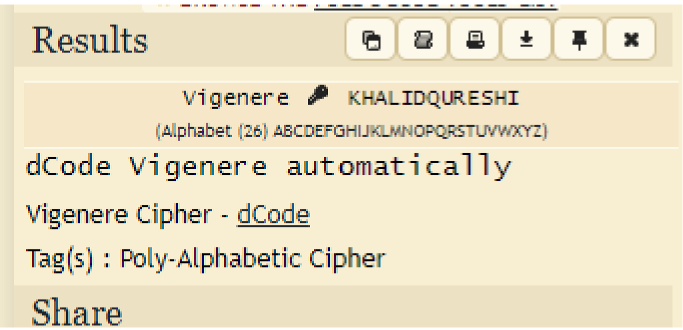
● Knowing the Key/Password: KHALIDQURESHI

○ 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)



Vigenere 🔑 KHALIDQURESHI
(Alphabet (26) ABCDEFGHIJKLMNOPQRSTUVWXYZ)

```
dCode Vigenere automatically
```

Vigenere Cipher - dCode

Tag(s) : Poly-Alphabetic Cipher

Conclusion:

In conclusion, while polyalphabetic ciphers like the Playfair and Vigenere ciphers offer more security than mono-alphabetic ciphers by using multiple alphabets, they are still vulnerable to cryptanalysis. Techniques such as Kasiski examination and frequency analysis adapted for polyalphabetic ciphers can break these encryption methods. Despite their increased complexity, they are not immune to systematic cryptanalysis, which can reveal the key or plaintext under certain conditions.