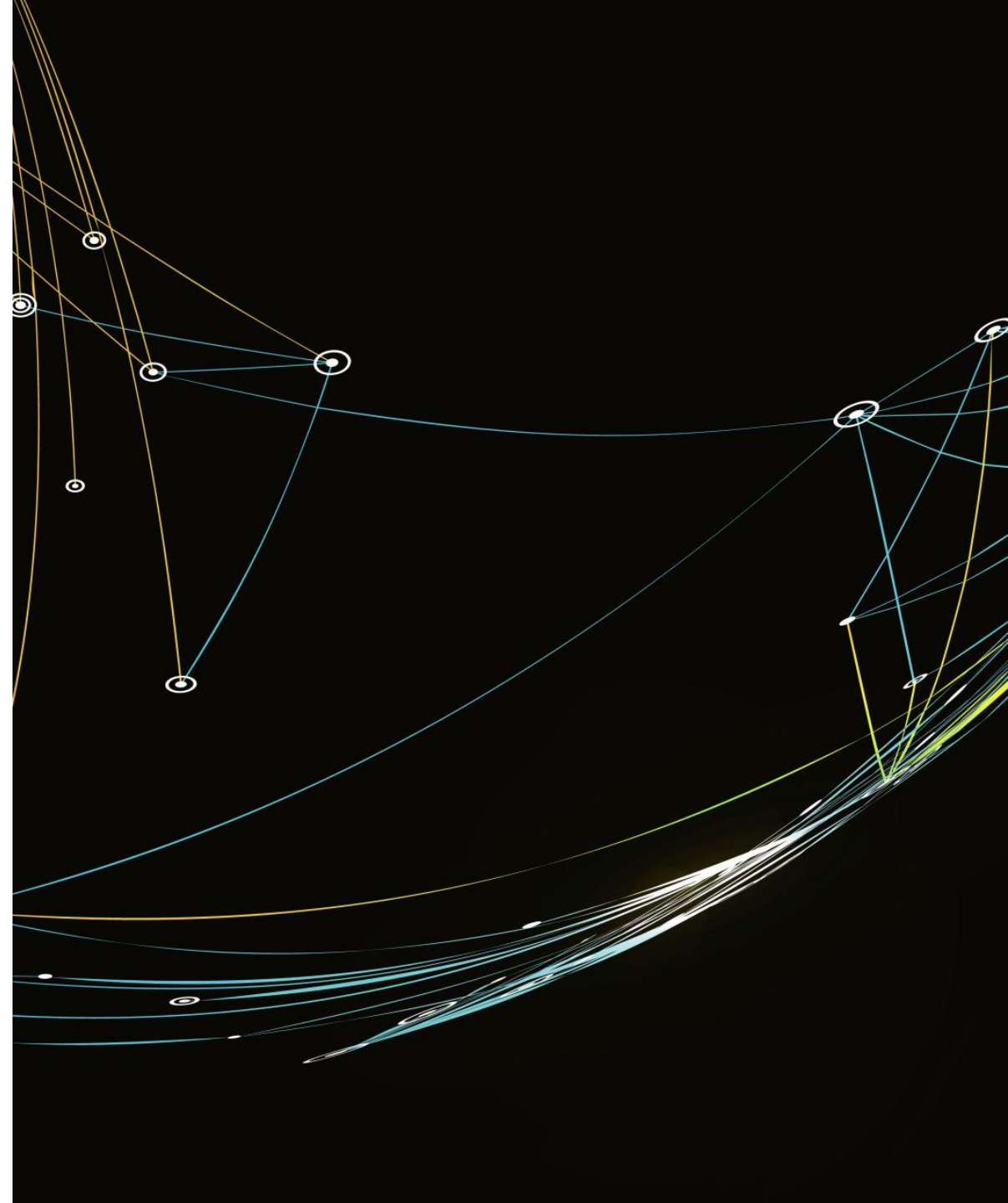

PROJECT

(Caesar Cipher – Playfair Cipher)



OVERVIEW

- This project is a simulation of two old cipher methods that applied on Text only.
- These two methods are :
 - Caesar Cipher
 - Playfair Cipher
- GitHub Repo : [GitHub Repo](#)

CAESER CIPHER

- Caesar used to encrypt his messages using a very simple algorithm, which could be easily decrypted if you know the key.
- He would take each letter of the alphabet and replace it with a letter at a certain distance away from that letter.
- Example with a shift of 3:

Text : ABCD
Encryption : DEFG
Decryption : ABCD

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

CAESER CIPHER

- You would use these Formulas to get the index of the wanted letter even in encryption or decryption
 - Encrypted letter = $(\text{plain letter index} + \text{key}) \bmod (\text{total number of letters})$
 - Decrypted letter = $(\text{cipher letter index} - \text{key} + \text{total number of letters}) \bmod (\text{total number of letters})$ - we add the total number of letters not to get a negative index
 - For English, this modulus (total number of letters) is 26.
-

CAESER CIPHER

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

Text = ABCD , Shift = 3

Encryption Formula = (plain letter index + key) mod (total number of letters)

Encryption letter index of (A) = $(0 + 3) \bmod (26) = 3$

Encryption letter = D

Encryption letter index of (B) = $(1 + 3) \bmod (26) = 4$

Encryption letter = E

Encryption letter index of (C) = $(2 + 3) \bmod (26) = 5$

Encryption letter = F

Encryption letter index of (D) = $(3 + 3) \bmod (26) = 6$

Encryption letter = G

Text Encrypted = DEFG|

CAESER CIPHER

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

Text = DEFG , Shift = 3

Decryption Formula = (cipher letter index - key + total number of letters) mod (total number of letters)

Decryption letter index of (D) = $(3 - 3 + 26) \bmod (26) = 0$

Decryption letter = A

Decryption letter index of (E) = $(4 - 3 + 26) \bmod (26) = 1$

Decryption letter = B

Decryption letter index of (F) = $(5 - 3 + 26) \bmod (26) = 2$

Decryption letter = C

Decryption letter index of (G) = $(6 - 3 + 26) \bmod (26) = 3$

Decryption letter = D

Text Decrypted = ABCD

PLAYFAIR CIPHER

- A 5X5 matrix of letters based on a keyword 1 fill in letters of keyword (No duplicates) 1 fill rest of matrix with other letters
- e.g. using the keyword MONARCHY

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

PLAYFAIR CIPHER

Text : BALLOON , Keyword : MONARCHY

pairs = BA , LX , LO , ON

BA (Same col) --> IB (shift down)

LX (differ row and col) --> SU (intersection row & col)

LO (differ row and col) --> PM (intersection row & col)

ON (Same row) --> NA (shift right)

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

Text Encrypted : IBSUPMNA

CAESER CIPHER - TASKS

1. Encrypt letter function
 2. Decrypt letter function
 3. Caesar Cipher Encrypt function
 4. Caesar Cipher Decrypt function
 5. Caesar Cipher function
 6. Input Functions
-

PLAYFAIR CIPHER - TASKS

1. Check letter function
 2. Unique Letters of keyword function
 3. Matrix function
 4. Text to pairs function
 5. Get index function
 6. String is alpha function
 7. Play Fair Encryption function
-

PLAYFAIR CIPHER - TASKS

1. Play Fair Decryption function
2. Play Fair function