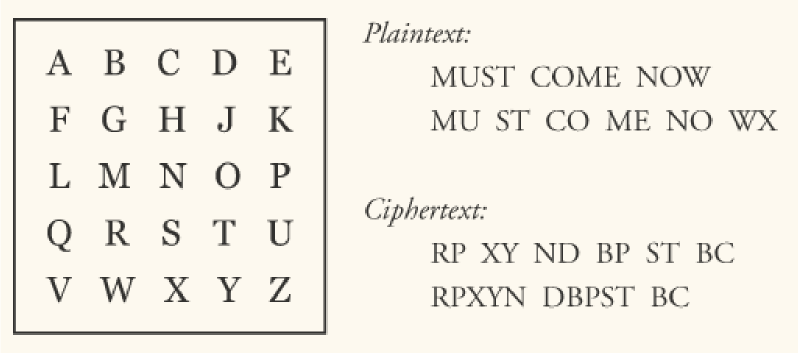
2477 - Introduction to Programming - Project Proposal
André Filipe Figueiredo Marques Silva - 26005

Ancient Cyphers for encrypting messages, through Python



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

Plaintext:
MUST COME NOW
MU ST CO ME NO WX

Ciphertext:
RP XY ND BP ST BC
RPXYN DBPST BC

Description

An encryption algorithm takes plain text and turns it into encrypted text. In order to decrypt it, one must have both the encrypted text *and* the key used in the encryption. These algorithms, thus, exist in pairs (encrypt + decrypt) and constitute the so-called **cyphers**.
Encryption has been around for a very long time, but many methods were particularly used during both World Wars. Even if nowadays these cyphers are obsolete due to computational power, they remain a good exercise for programming beginners.

Objectives

1. Construct an original modification of a known cypher – the Polybius Square. What this means is: my cypher will be based on it but will have some kind of modification that forces me to code it from scratch.
2. Proceed to implement that modified cypher through Python, developing both the encrypt and decrypt algorithms.
3. Get the algorithms to accept simple inputted text as a first step, and then build on to letting them accept .txt files directly.
4. Implement all of this as an executable script format that can be run from a terminal and generates an encrypted file.

Specific Functionality

User inserted plain text or .txt file	Second algorithm for reversing the process
Transform into encrypted text	Making it “appealing”, even if in a geek way
Return encrypted text/file to the user	Implement all of this, but through a script
Return encoding key to the user	