Individual Project

Class	GEMATMW
Created	@Jan 6, 2021 9:24 PM
Discussed / Given	
Materials	This is a CLI Application coded in the Go Programming Language \ for my 1st term university project in GEMATMW(Mathematics in the Modern World) at De La Salle University Manila. \ This program will consist of different functions that can \ encrypt and decrypt messages.
Module	
Related	Mathematics in Digital Communications
Related to MES Tasks	
Reviewed	☐
Type	Project
Week	11

▼ Table of Contents

```
func affineCipher(...param)
func atbashCipher(...param)
func shiftCipher(...param)
func vigenereCipher(...param)
func railFenceCipher(...param)
func rsaCipher(...param)
```

Introduction

> This is a CLI Application coded in the Go Programming Language for my 1st term university project in GEMATMW (Mathematics in the Modern World) at De La Salle University Manila. This program will consist of different functions that can encrypt and decrypt messages. This is was made with the Commando package.

How To

Command Format

```
$ ciphers [ciphersystem] [message] -k [key] -p [encrypt|decrypt]
OUPUT
```

$Ciphersystem$	Key
$affine$	$\mathbb{N},\mathbb{N}$
$atbash$	n/a
$shift$	$\mathbb{N}$
$vigenere$	$string$
$rail$	$\mathbb{N}$
rsa	$\mathbb{N},\mathbb{N}$

```
EXAMPLES
$ ciphers affine "This is the message" -key 1,2 -process encrypt
$ ciphers shift "Another message" -k 10
BY DEFAULT, ALL OF THESE ARE ENCRYPTION
$ ciphers vigenere "Aries Vince" -key "hello there" -p decrypt
```

Cipher Functions

*Each alphabet character is mapped as A-0, B-1, C-2, D-3, ..., & Z-25. Upper and lowercase is handled and spaces are left in-place except for rail fence cipher.

`func affineCipher(...param)`

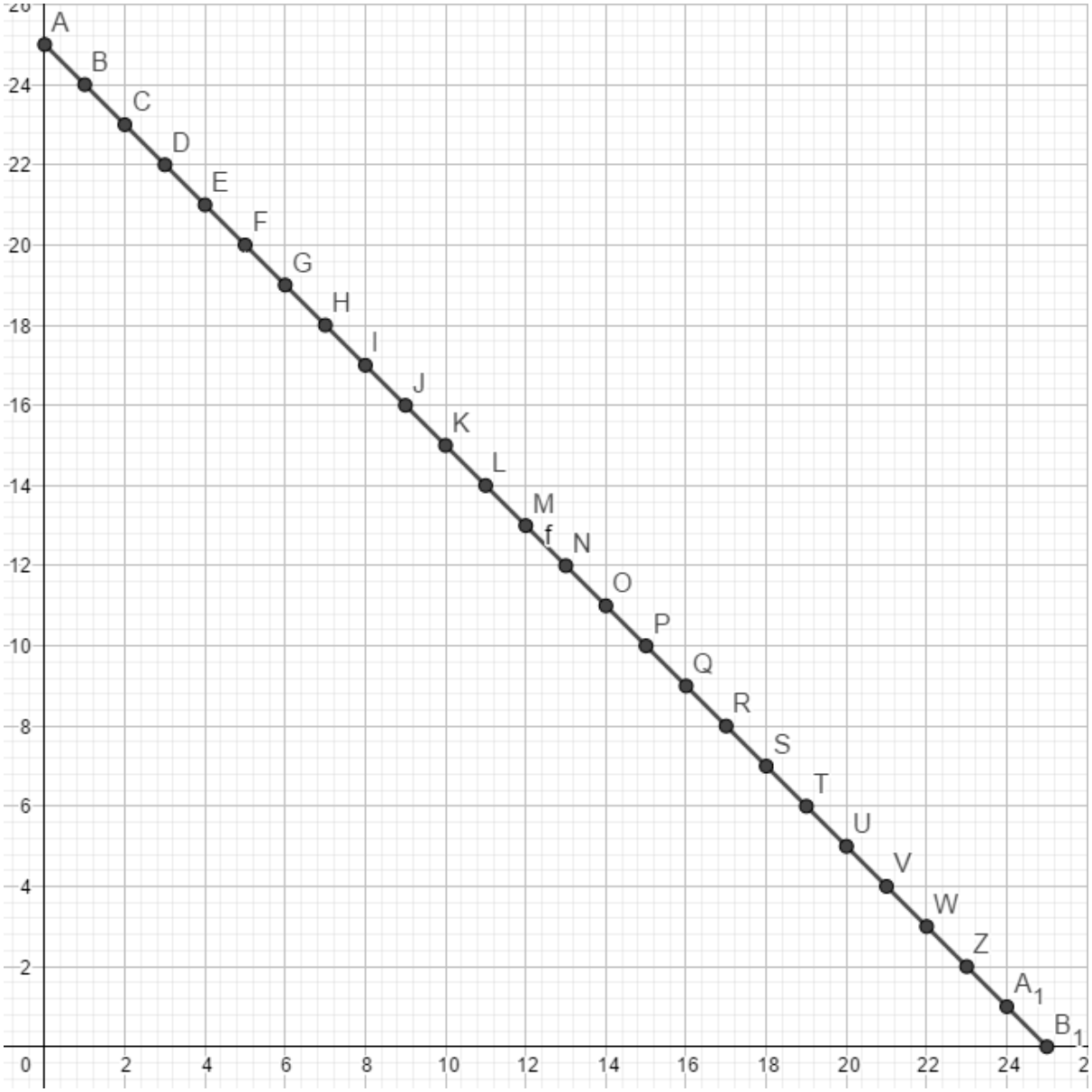
The affine cipher is an encryption of the form:

$$E(x) = (ax + b) \mod 26$$

and decryption is as simple as solving for x:

$$D(x) \equiv a^{-1}(y - b) \mod 26$$

`func atbashCipher(...param)`



By plotting (input,output) for the atbash cipher from 0-25, we get:

$$E(x) = (-x + 25) \mod 26$$

`func shiftCipher(...param)`

$$E(x) = (x) \mod 26$$

This is the encryption formula based on the affine cipher previously mentioned. Each character is shifted linearly left or right.

`func vigenereCipher(...param)`

For each character of the message an output is determined by shifting the alphabet letter a certain number of steps using a given string type key. Unlike the the shift cipher each character is shifted according to a different shift key, thus harder to crack without the key.

`func railFenceCipher(...param)`

The rail fence creates an array-like rows and columns where each character is mapped as so: (Example)

	0	1	2	3	4	5	6	7	8	9	10
1	f						p				
2		e						e			
3			l		x				w		s
4				i						d	

where the key is the number of rows used, and the columns are determined by the number of characters in the message processed. From top-left going right, each character passed that is in the diagonals is added to the message, becoming: "fpe elxwsid".

`func rsaCipher(...param)`