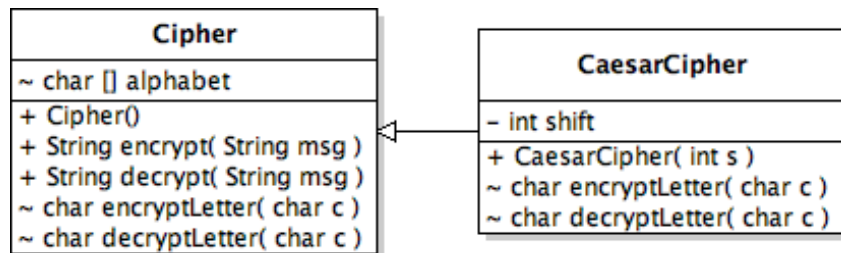# CECS 277 – Lab 6

Secret Decoder Ring

Write a program that allows the user to encrypt or decrypt messages using different types of encryption methods. Ask the user whether they want to encrypt or decrypt a message, if they choose encrypt, prompt them to type in a message and to choose an encryption type, Atbash, or Caesar, if they choose Caesar, prompt them for a shift amount (1-25). Encrypt the message and write it to a file called 'message.txt' (leave any spaces or punctuation the same). If they choose to decrypt, prompt them to choose a decryption type, and a shift amount if they choose Caesar. Decrypt the message read in from the 'message.txt' file and display it to the screen.

Implement the following class structure for your program, please do not add to or modify the class structure. The encrypt/decrypt methods in the Cipher class should loop through the message and call encryptLetter/decryptLetter for each character in the string. The EncryptLetter/decryptLetter in the Cipher class should use the Atbash Cipher, encryptLetter/decryptLetter in the CaesarCipher class should use the Ceasar Cipher. (+ is public, ~ is protected, - is private):

```
                Cipher
~ char [] alphabet
+ Cipher()
+ String encrypt( String msg )
+ String decrypt( String msg )
~ char encryptLetter( char c )
~ char decryptLetter( char c )
```

```
            CaesarCipher
- int shift
+ CaesarCipher( int s )
~ char encryptLetter( char c )
~ char decryptLetter( char c )
```

<u>Atbash Cipher</u> – is a simple substitution cipher where the encrypted message is obtained by looking up each letter and finding the corresponding letter in a reversed alphabet. The encoded letter can be found in one of two ways, parallel array lookup (ex. letter to encode = 'B', location = 1, encoded letter location = 1, which is a 'Y') or calculated (ex. letter to encode = 'B', location = 1, 25 – location = 24, encoded letter location = 24, which is a 'Y').

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

<u>Caesar Cipher</u> – is another substitution cipher where the encrypted message is obtained by looking up each letter and finding the corresponding letter in a shifted alphabet (ex. letter to encode = 'B', location = 1, location + shift value = 1+3, encoded letter location = 4, which is an 'E'). If the shift value goes past the end of the alphabet, then it should wrap around to the beginning (ex. letter to encode = 'X', location = 23, location + shift value = 23+3, encoded letter location = 26, which is larger than 25, subtract off the number of letters to get the updated location = 0, which is an 'A').

Example: shift = 3:

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
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

Example Output:

```
Secret Decoder Ring:
1. Encrypt
2. Decrypt
1
Enter Encryption Type:
1. Atbash
2. Caesar
2
Enter message: THE SOUP IS POISONED
Enter shift value: 3
Encrypted message saved to "message.txt".
```

Encrypted message written to file: `WKH VRXS LV SRLVRQHG`

```
Secret Decoder Ring:
1. Encrypt
2. Decrypt
2
Enter Decryption Type:
1. Atbash
2. Caesar
2
Reading encrypted message from "message.txt".
Enter shift value: 3
Decrypted Message: THE SOUP IS POISONED
```