ATBASH CIPHER UI

Problem Statement- **Write a program with a nice UI to Encipher /Decipher with the Atbash encryption algorithm.**

Theory - **The Atbash Cipher was originally a monoalphabetic substitution cipher used for the Hebrew alphabet. It is one of the earliest known substitution ciphers to have been used, and is very simple. The Atbash Cipher simply reverses the plaintext alphabet to create the ciphertext alphabet. That is, the first letter of the alphabet is encrypted to the last letter of the alphabet, the second letter to the penultimate letter and so forth.**

For the Roman alphabet of 26 letters, we have the ciphertext alphabet as given in the table below.

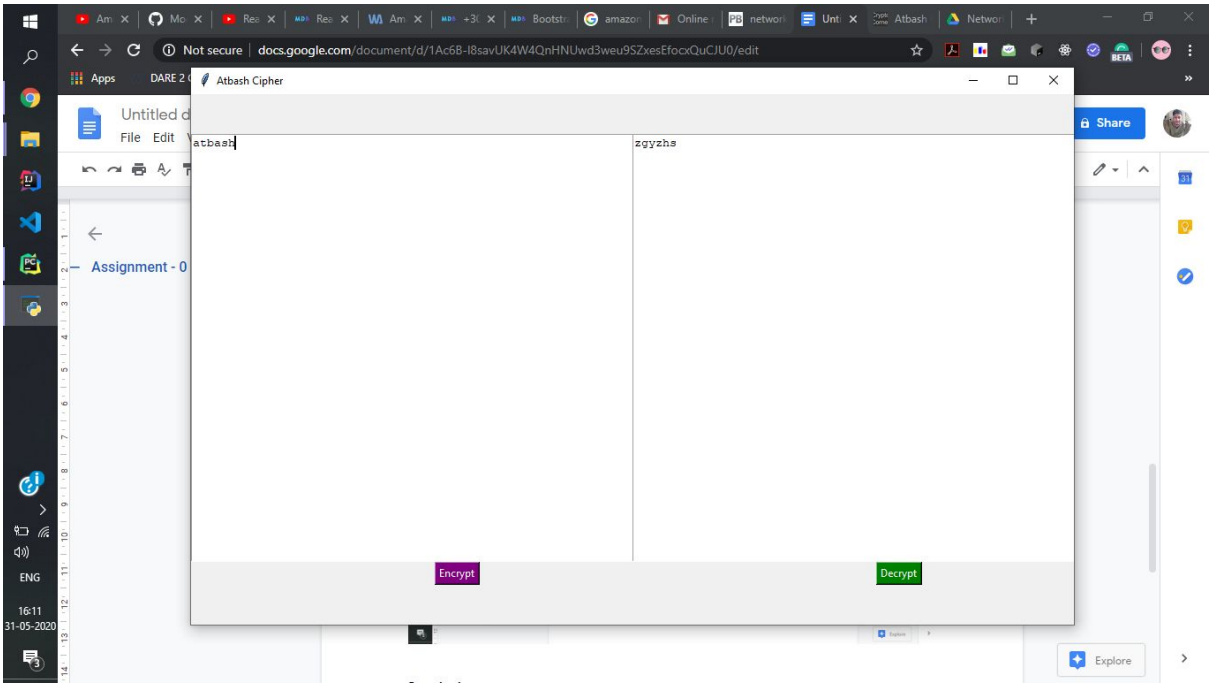
Plaintext Alphabet	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext Alphabet	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A

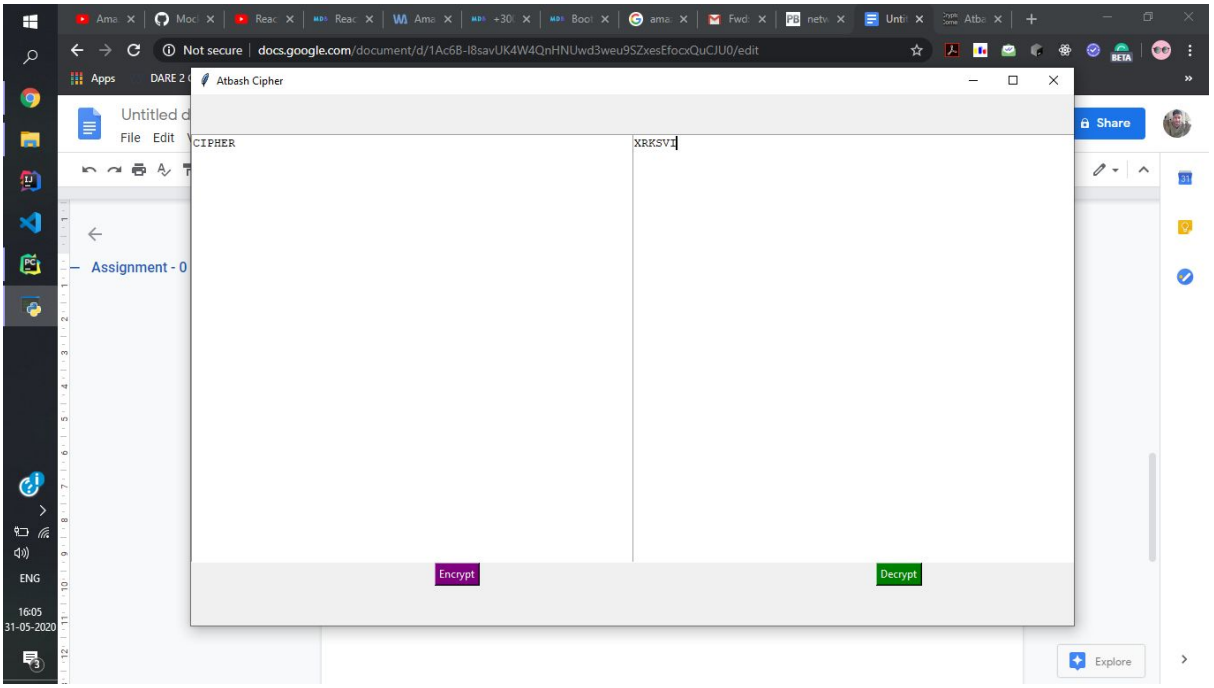
Encryption **- As with any monoalphabetic substitution cipher, encryption using the Atbash Cipher is very simple once the ciphertext alphabet has been generated. We simply replace each occurence of each plaintext letter with the respective ciphertext letter given by the table. So, if we take the plaintext "atbash", we can see that "a" enciphers to "Z", "t" enciphers to "G" and so on. Continuing in this way, we see that the final ciphertext is "ZGYZHS".**

Decryption **- Due to the symmetric nature of this cipher, the decryption process is exactly the same as the encryption process. Thus, for the recipient to decrypt the ciphertext, the same ciphertext alphabet must be generated as was used to encrypt the message in the first place. In this case, the ciphertext alphabet relies only on the alphabet used, and hence the table above is also used to decipher the message. So, given the ciphertext "XRKSVI", and assuming that the alphabet used was the standard Roman alphabet of 26 letters, we can retrieve the plaintext "cipher".**

Code Link -
https://drive.google.com/file/d/1egaF3c-eVFfeJr1cko8BNaPoC1JpV8TA/view?usp=sharing

Screenshots-





Conclusion - **The Atbash Cipher is a very weak substitution cipher, since there is no secret key behind generating the ciphertext alphabet to perform the encryption. Thus, given a piece of ciphertext, known to have been enciphered using the Atbash Cipher, anyone who intercepts the message can easily decipher it to retrieve what was meant to be concealed.**

Despite this, it provides a very quick and easy way to conceal messages from an onlooker and can be used successfully to encipher messages of not great importance.