One Time Pad

APPLIED CRYPTOGRAPHY

AARYA ARUN	PES1201700009
MANEESHA S	PES1201700024
INDU RALLABHANDI	PES1201700795

What is one time pad?

- The One Time Pad is an encryption technique that cannot be cracked.
- A one time pre-shared key is required, which has to be of the same length or greater length than the message.
- It must be ensured that the key is truly random and is confidential between the sender and the receiver from which uncrackable security can be achieved.
- This key is destroyed by the sender and the receiver after use.

CIPHER MECHANISM

ENCRYPTION:

- *Every character from the plaintext and the key are converted into their 8-bit binary equivalents.*

- *Then, bitwise XOR operation is performed between the corresponding bits of the plaintext and key which provides a result with the number of bits equal to that of the binary equivalent of the key. This is the ciphertext.*

- *On grouping every 8-bits of the binary result obtained(ciphertext) and converting them back to characters we arrive at a readable form of the ciphertext.*

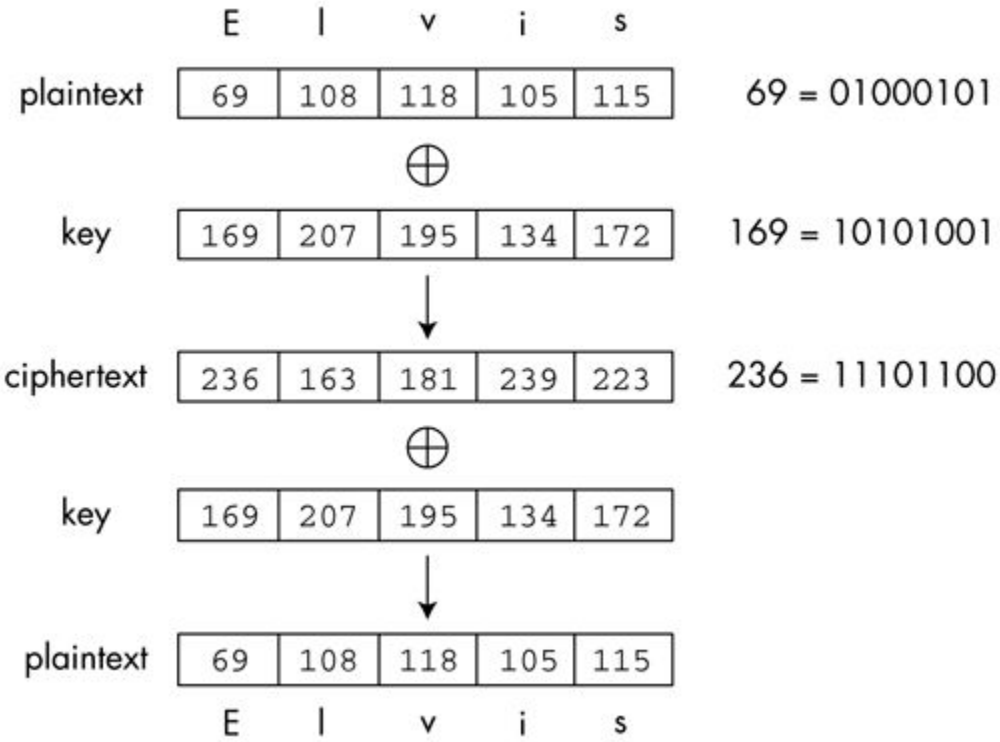
DECRYPTION:

- *Every character from the ciphertext and the key are converted into their 8-bit binary equivalents.*

- *Then, bitwise XOR operation is performed between the corresponding bits of the ciphertext and key which provides a result with the number of bits equal to that of the binary equivalent of the key. The result obtained is the plaintext that was encoded.*

- *On grouping every 8-bits of the binary plaintext and converting them back to characters we arrive at a readable form of the plaintext.*

CIPHER MECHANISM



	E	l	v	i	s	
plaintext	69	108	118	105	115	69 = 01000101
			⊕			
key	169	207	195	134	172	169 = 10101001
			↓			
ciphertext	236	163	181	239	223	236 = 11101100
			⊕			
key	169	207	195	134	172	
			↓			
plaintext	69	108	118	105	115	
	E	l	v	i	s	

INPUT

- Mode: Indicates whether you are encrypting or decrypting the given message. (as there is a difference in the way the message is displayed depending on the function being called)

- Text: This could be your plaintext or ciphertext depending on the mode specified.

- Key: The key used for encryption/decryption.

OUTPUT

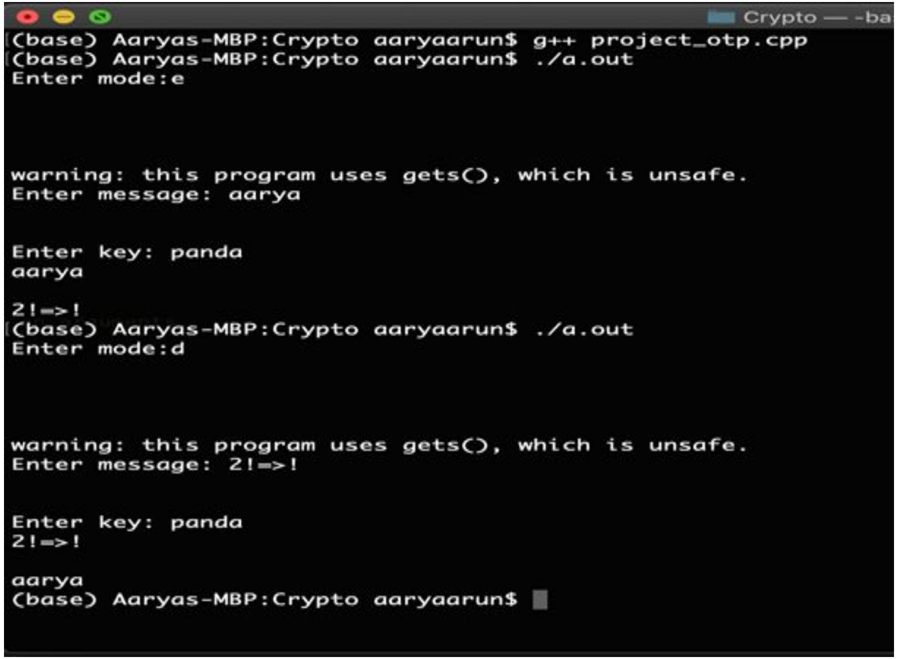
- Text: Outputs the given text.

- Encrypted/decrypted text: Based on the mode, the encrypted/decrypted text is printed.

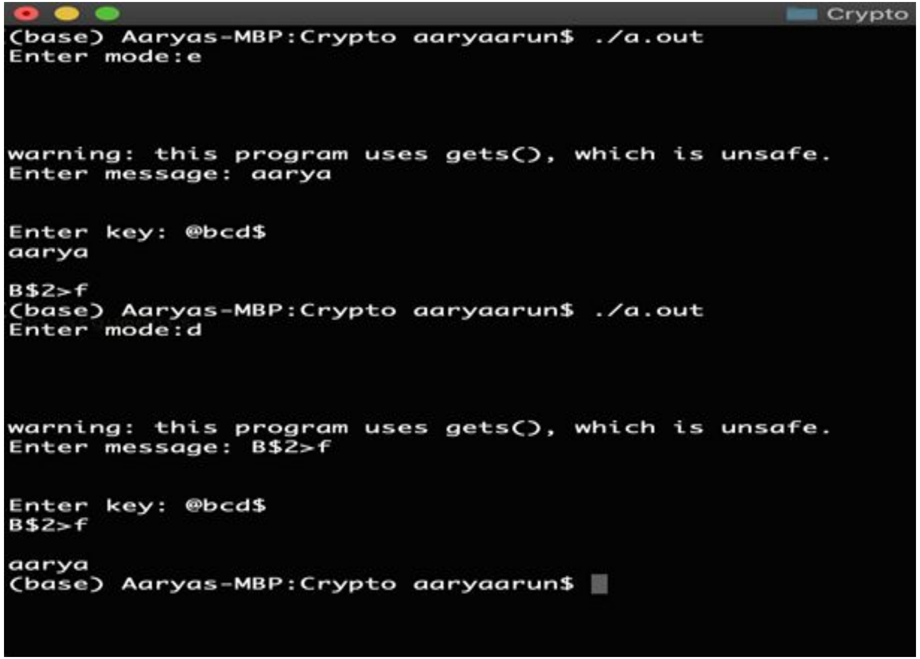
CODE MECHANISM

- The user inputs a mode (‘e’ for encryption mode and ‘d’ for decryption mode).
- The code checks whether an acceptable mode has been provided as input.
- The user provides the inputs in the form of strings (signed characters).
- The code checks whether the key length and message length are compatible (i.e. they match).
- In order to perform smooth bitwise operation, the characters are converted to unsigned characters.
- A bitwise XOR operation is performed on the key and text provided to obtain the encrypted/decrypted text.
- The output is shown as text for the ease of readability. (eliminating the possibility of having unprintable characters)

Output Screenshots



```
(base) Aaryas-MBP:Crypto aaryaarun$ g++ project_otp.cpp
(base) Aaryas-MBP:Crypto aaryaarun$ ./a.out
Enter mode:e




warning: this program uses gets(), which is unsafe.
Enter message: aarya


Enter key: panda
aarya

2!=>!
(base) Aaryas-MBP:Crypto aaryaarun$ ./a.out
Enter mode:d




warning: this program uses gets(), which is unsafe.
Enter message: 2!=>!


Enter key: panda
2!=>!

aarya
(base) Aaryas-MBP:Crypto aaryaarun$
```



```
(base) Aaryas-MBP:Crypto aaryaarun$ ./a.out
Enter mode:e




warning: this program uses gets(), which is unsafe.
Enter message: aarya


Enter key: @bcd$
aarya

B$2>f
(base) Aaryas-MBP:Crypto aaryaarun$ ./a.out
Enter mode:d




warning: this program uses gets(), which is unsafe.
Enter message: B$2>f


Enter key: @bcd$
B$2>f

aarya
(base) Aaryas-MBP:Crypto aaryaarun$
```

Merits

- Provides the security of a one time pad.
- Has encryption and decryption mode which is accurate given the constraints.
- Does work when special characters are included in the key or plaintext.
- Simple logic yet secure.

ConstraInts

- The size of the message cannot be more than 10000 characters.
- We cannot give texts that include newline characters.

Further scope of the project

To allow input in the form of a text file and compute cipher text even if the message contains newline characters and large message sizes.

Code

The code has been uploaded on GitHub and can be accessed through the following link:

GITHUB LINK:

https://github.com/aarya-arun/Cryptography/tree/master/One%20Time%20Pad

THANK YOU