****

**PROGRAMMING C++**

**FINAL PROJECT**

**(ENCRYPTION & DECRYPTION)**

**LECTURER’S NAME: EN. MUHAMMAD ADIB BIN IZZUDIN**

**SECTION: 39**

**GROUP MEMBERS:**

1. **AHMAD FAHMI BIN AZLAN @ AZLAN AMIN A17DW4144**
2. **NUR AQILAH SYAHIRAH BINTI JAYEN @ SUPAAT A17DW2330**

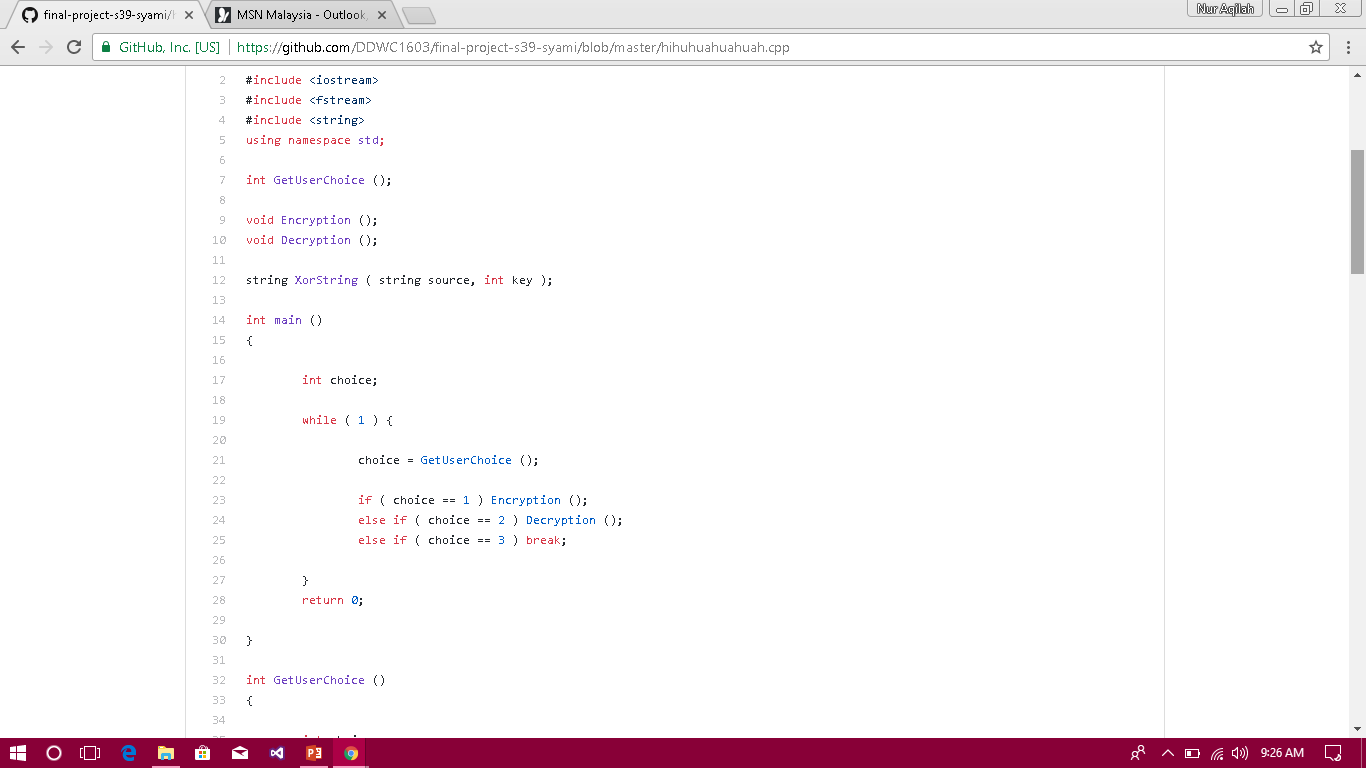
**INTRODUCTION.**

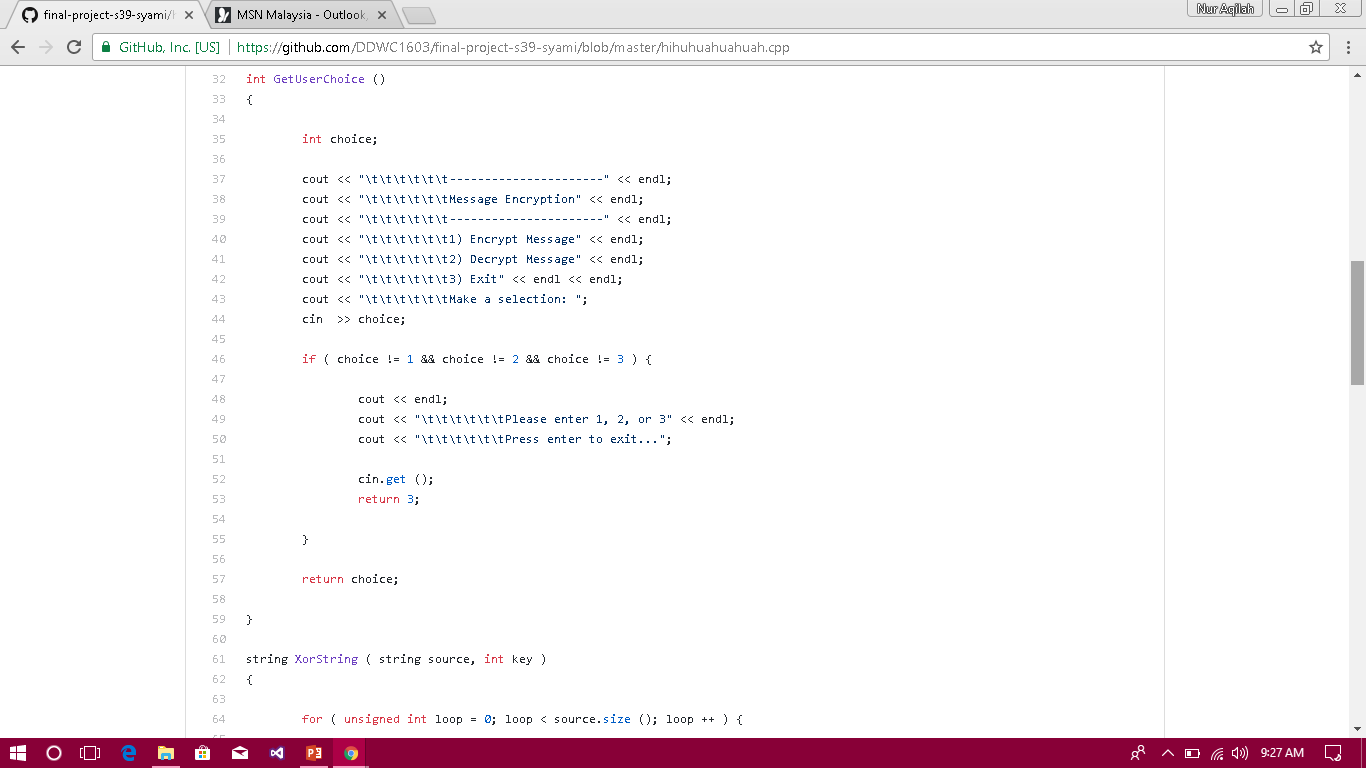
Encryption is the process of using an algorithm to transform information to make it unreadable for unauthorized users. This cryptographic method protects sensitive data such as credit card numbers by encoding and transforming information into unreadable cipher text. This encoded data may only be decrypted or made readable with a key. Symmetric-key and asymmetric-key are the two primary types of encryption. Decryption is the process of transforming data that has been rendered unreadable through encryption back to its unencrypted form. In decryption, the system extracts and converts the garbled data and transforms it to texts and images that are easily understandable not only by the reader but also by the system. Decryption may be accomplished manually or automatically. It may also be performed with a set of keys or passwords. One of the foremost reasons for implementing an encryption-decryption system is privacy. As information travels over the World Wide Web, it becomes subject to scrutiny and access from unauthorized individuals or organizations. As a result, data is encrypted to reduce data loss and theft. Some of the common items that are encrypted include email messages, text files, images, user data and directories. The person in charge of decryption receives a prompt or window in which a password may be entered to access encrypted information. In our program, we used caser cypher to encrypt and decrypt the text. The Caesar cipher is one of the earliest known and simplest ciphers. It is a type of substitution cipher in which each letter in the plaintext is 'shifted' a certain number of places down the alphabet. For example, with a shift of 1, A would be replaced by B, B would become C, and so on. The method is named after Julius Caesar, who apparently used it to communicate with his generals. More complex encryption schemes such as the [Vigenère](http://www.practicalcryptography.com/ciphers/classical-era/vigenere-gronsfeld-and-autokey/) cipher employ the Caesar cipher as one element of the encryption process. The widely known ROT13 'encryption' is simply a Caesar cipher with an offset of 13. The Caesar cipher offers essentially no communication security, and it will be shown that it can be easily broken even by hand.

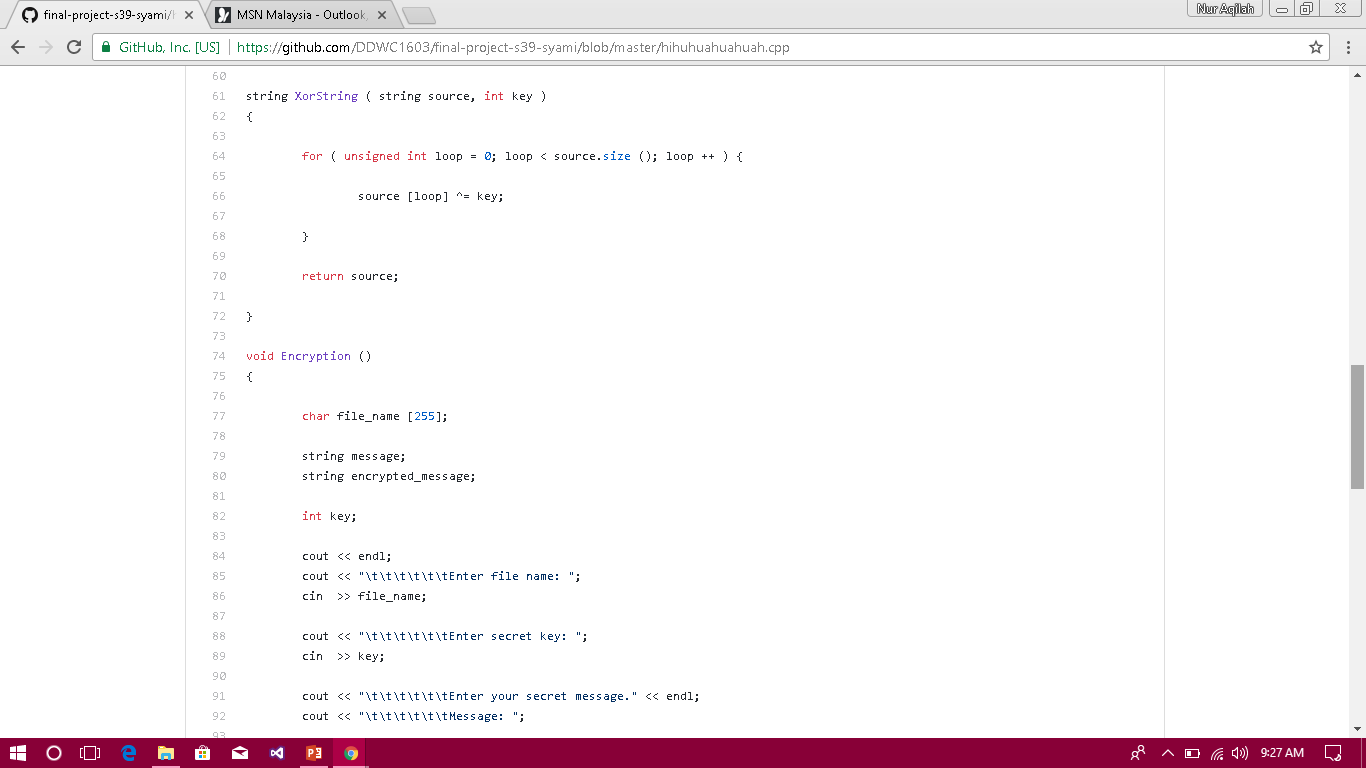
**OBJECTIVE.**

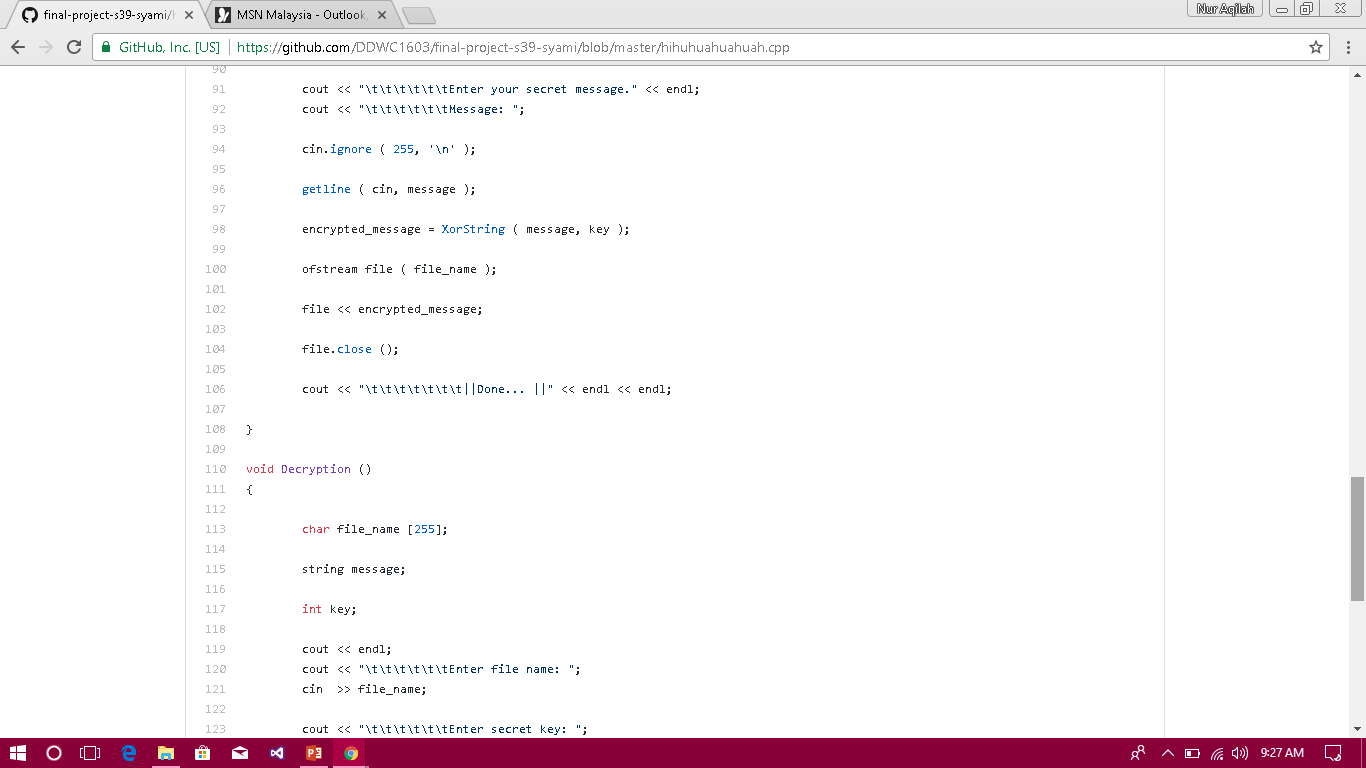
First of all, encryption provides security for data at all times. Generally, data is most vulnerable when it is being moved from one location to another. Encryption works during data transport or at rest, making it an ideal solution no matter where data is stored or how it is used. Encryption should be [standard for all data](https://www.smartdatacollective.com/data-protection-different-ways-hackers-attack/) stored at all times, regardless of whether or not it is deemed “important”. Next, encrypted data maintains integrity. It is because hackers don’t just steal information, they also can benefit from altering data to commit fraud. While it is possible for skilled individuals to alter encrypted data, recipients of the data will be able to detect the corruption, which allows for a quick response to the cyber-attack. Encryption can protect the privacy as it is used to [protect sensitive data](https://www.schneier.com/blog/archives/2015/06/why_we_encrypt.html), including personal information for individuals. This helps to ensure anonymity and privacy, reducing opportunities for surveillance by both criminals and government agencies. Encryption technology is so powerful that some governments are attempting to put limits on the effectiveness of encryption which does not ensure privacy for companies or individuals. Encryption is also a part of compliance as many industries have strict compliance requirements to help protect those whose personal information is stored by organizations. HIPAA, FIPS, and other regulations rely on security methods such as encryption to protect data, and businesses can use encryption to achieve [comprehensive security](http://cjdegreeonline.bu.edu/protecting-your-identity-from-growing-cyber-crime-threats/). Lastly, encryption can protect data across the devices. Multiple (and mobile) devices are a big part of our lives, and transferring data from device to device is a risky proposition. Encryption technology can help protect store data across all devices, even during transfer. Additional security measures like advanced authentication help deter unauthorized users.

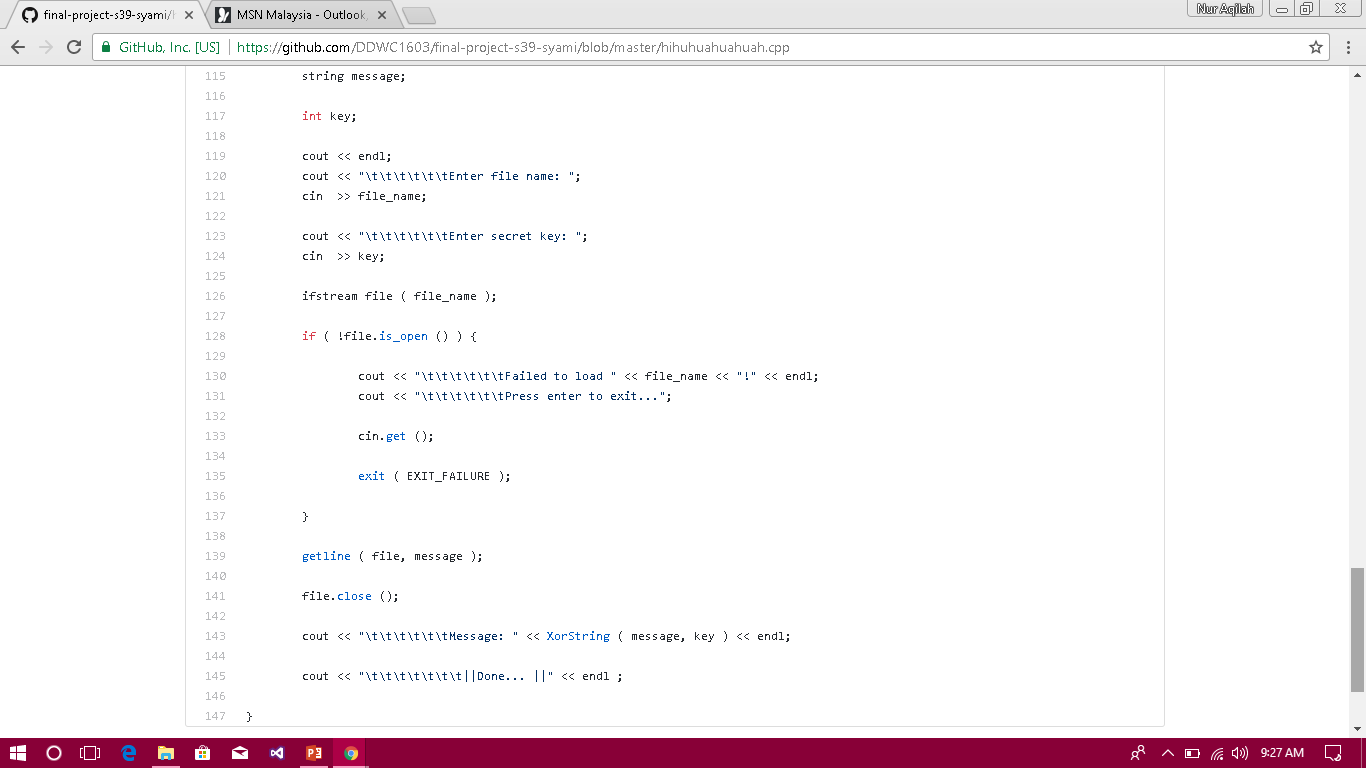
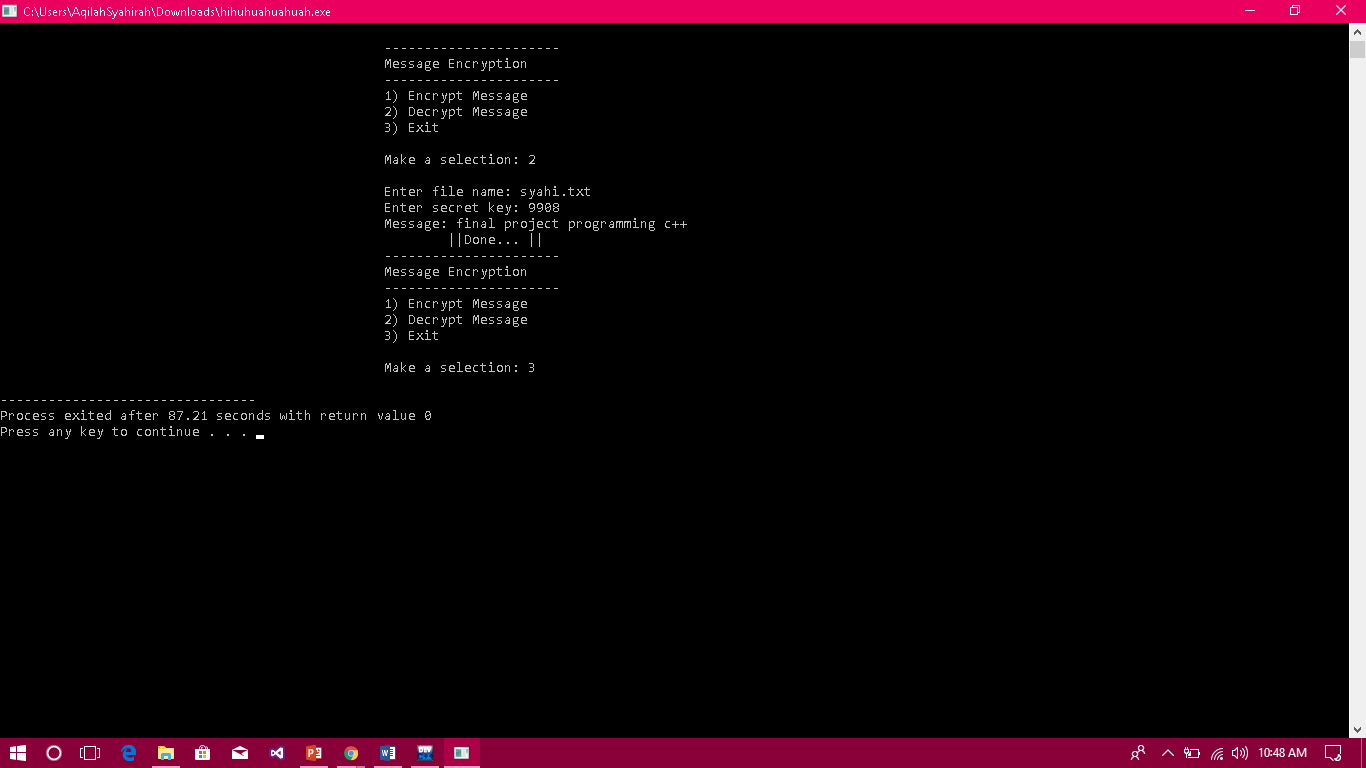
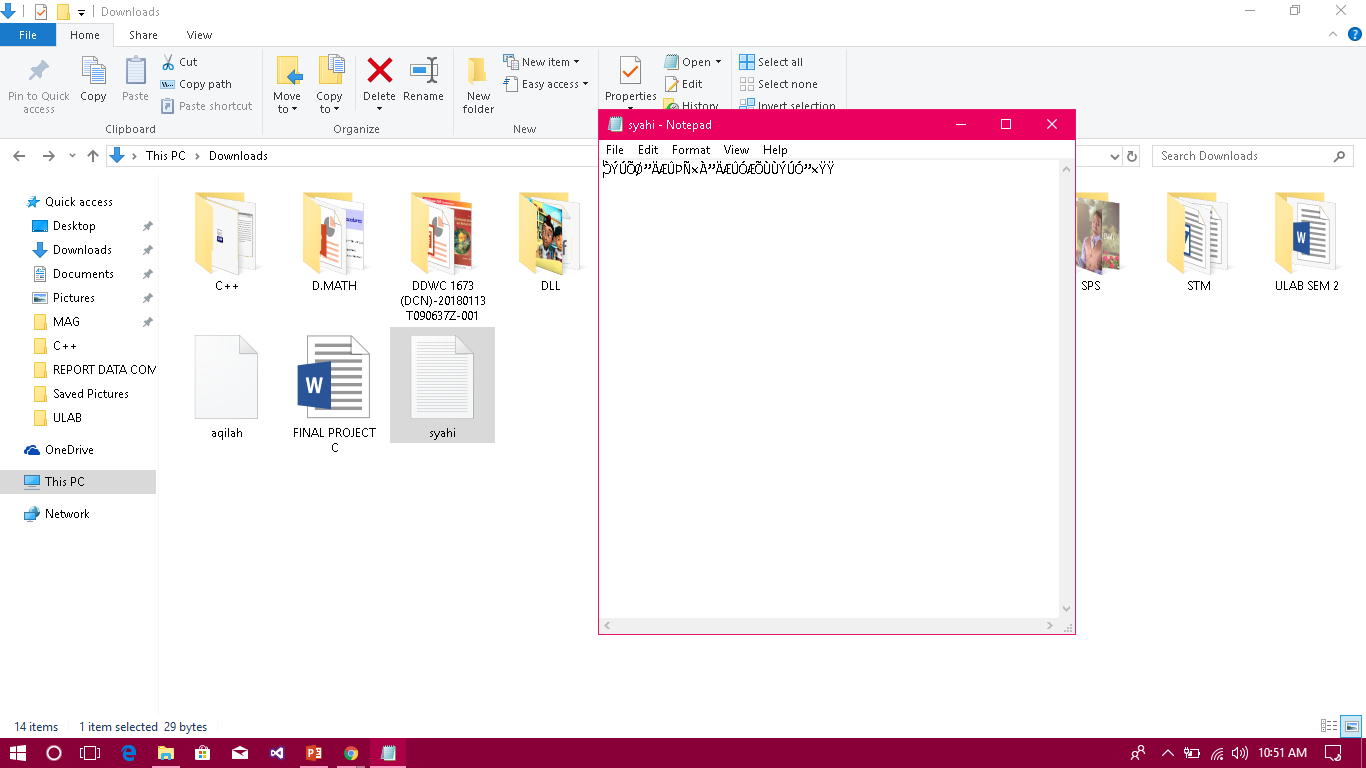
**CODING.**

****

****

****

****

******OUTPUT.**

**FLOW CHART.**

Display the secret message

Insert the secret key

Insert file name

Insert the secret message

Insert the secret key

Insert file name

Choose

**CONCLUSION.**

In conclusion, encryption and decryption of data give us many benefits as it can increase the security of our file or the message that we want to deliver to someone. If you use this program, your data will secure from other people. The other advantage can we get when we used this encryption and decryption program are you can avoid the hacker to hack or take your important file as they didn’t know your secret key. The secret key is really important in this case, because if you forget your secret key, the program will not open the file for you and you will not know the secret message that you have enter in this program. In my opinion, this program is very rational to use especially when we want to save the important and private file. I can say that the purpose of encryption and decryption program is all about to increase the security level and give the protection to our file.