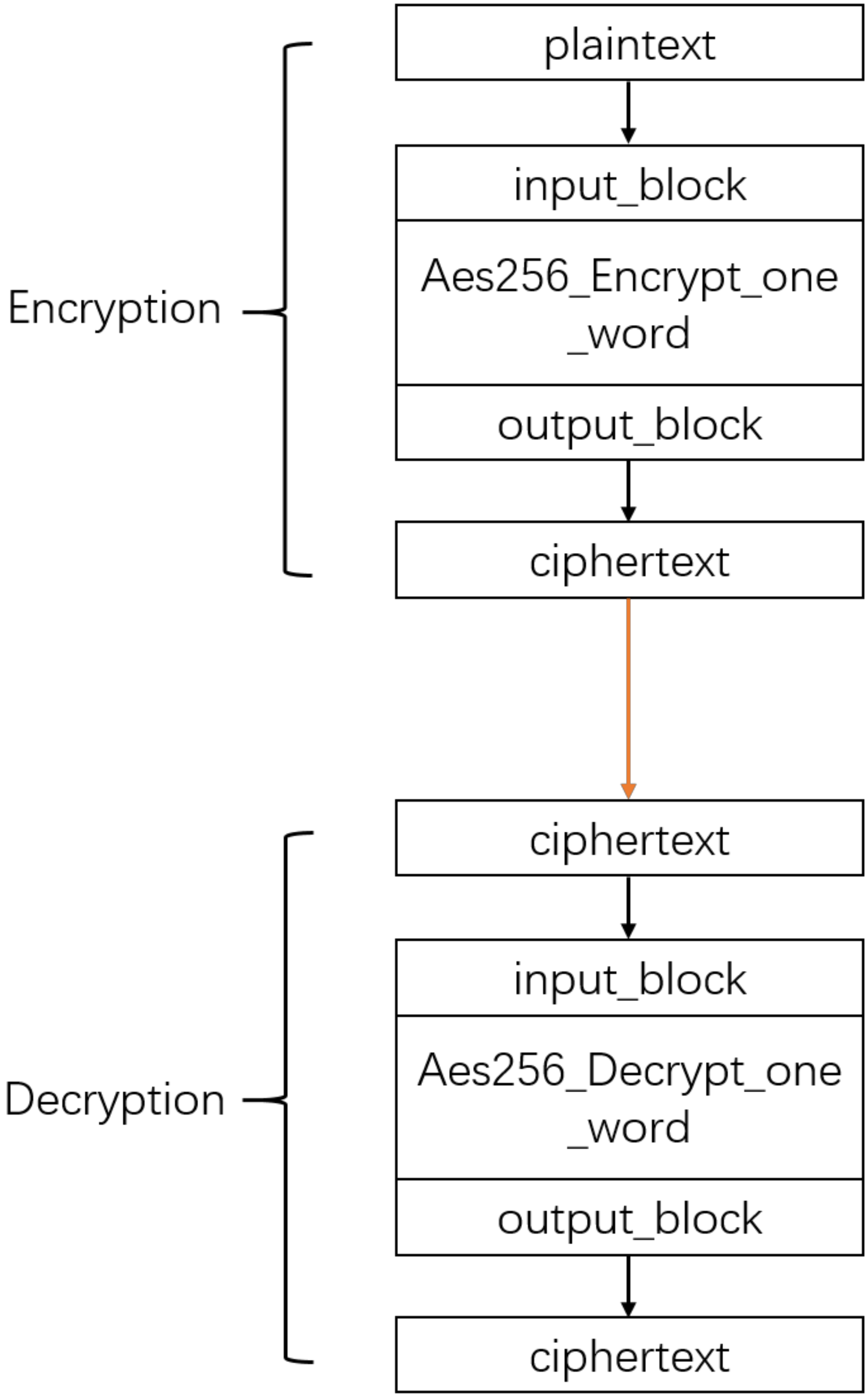
REPORT

Computer and Network Security

Project : Ransomware

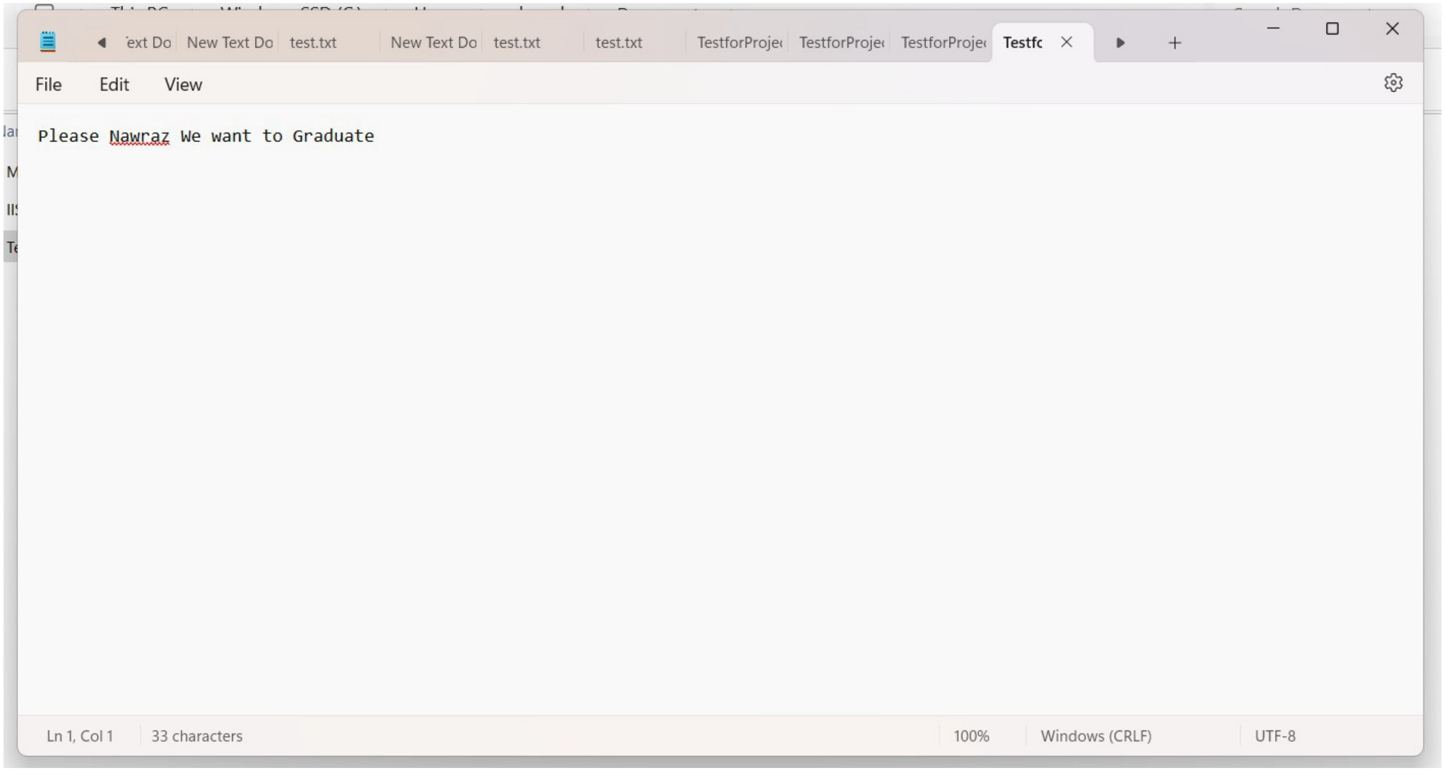

plaintext
input_block
Aes256_Encrypt_one_word
output_block
ciphertext
Encryption
ciphertext
input_block
Aes256_Decrypt_one_word
output_block
ciphertext
Decryption

The Electronic Codebook (ECB) mode is a fundamental block cipher mode used in encryption that processes data in fixed-size blocks. In **ECB mode**, each block of plaintext is independently encrypted using the ***Advanced Encryption Standard (AES) algorithm***, producing a corresponding block of ciphertext. This mode does not involve any interaction or dependency between blocks, making it a straightforward and easy-to-implement encryption method. ECB mode serves the primary function of ensuring confidentiality by converting plaintext into ciphertext. This is accomplished by applying the AES algorithm to each individual data block with a symmetric encryption key. The AES algorithm employs a substitution-permutation network to execute a series of mathematical transformations on each input block, resulting in a transformed ciphertext block. This process is repeated for every block of data, continuing until the entire message is encrypted.

One of the key advantages of ECB mode is its *simplicity and efficiency*. Since each block is processed independently, it allows for parallel encryption and decryption, making it easy to implement across various platforms. However, this independence also introduces a significant vulnerability: identical plaintext blocks result in identical ciphertext blocks, potentially revealing patterns and compromising the confidentiality of the data. Due to this vulnerability, ECB mode is not recommended for encrypting large datasets or data with repetitive patterns.
To address these security concerns, alternative encryption modes such as ***Cipher Block Chaining (CBC) or Counter (CTR) are often preferred***. These modes introduce additional operations, such as XORing plaintext with previous ciphertext blocks or using a counter, to enhance randomness and mitigate the vulnerabilities inherent in ECB mode.

In conclusion, **ECB mode in AES encryption** functions by independently transforming plaintext blocks into ciphertext, providing basic confidentiality. However, its limitations and potential vulnerabilities must be carefully considered when selecting an encryption scheme for specific applications.

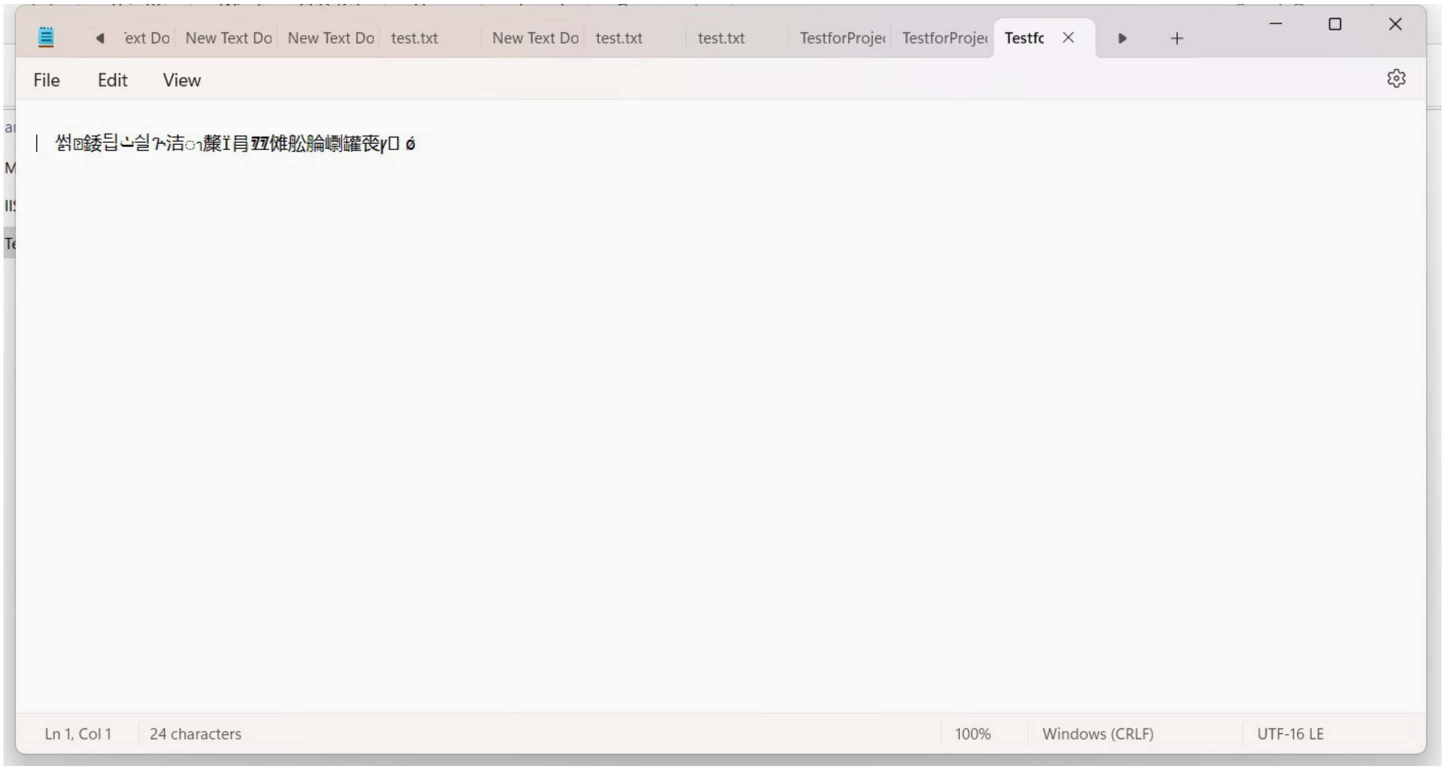
The Text File before encryption :-



```
Please Nawraz We want to Graduate
```

Ln 1, Col 1 | 33 characters | 100% | Windows (CRLF) | UTF-8

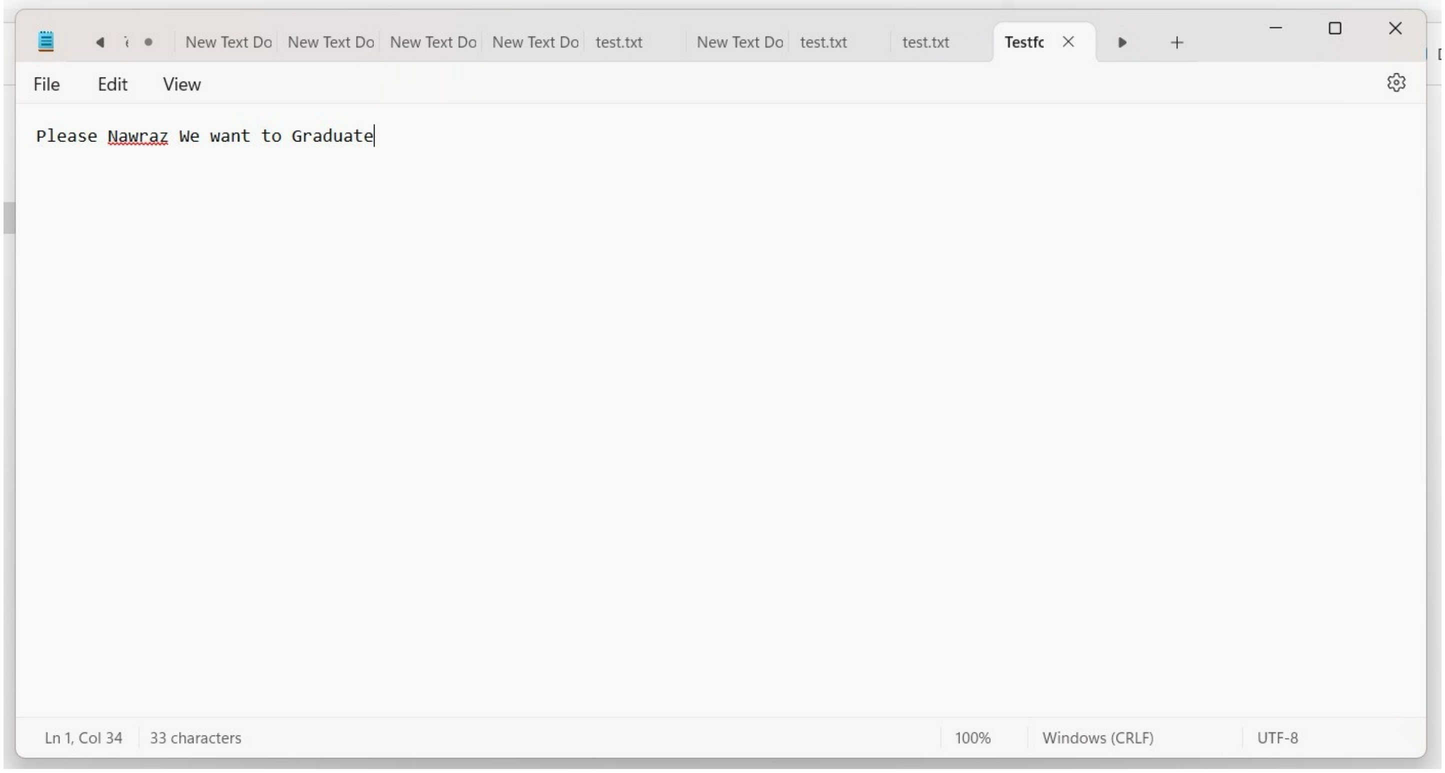
The Text File after encryption :-



```
쌝⊡銹딥ـ실ᡏ洁○ㅣ蘩Ï肙ꝏ傩舩艙噅罐丧ɣ□ ǿ
```

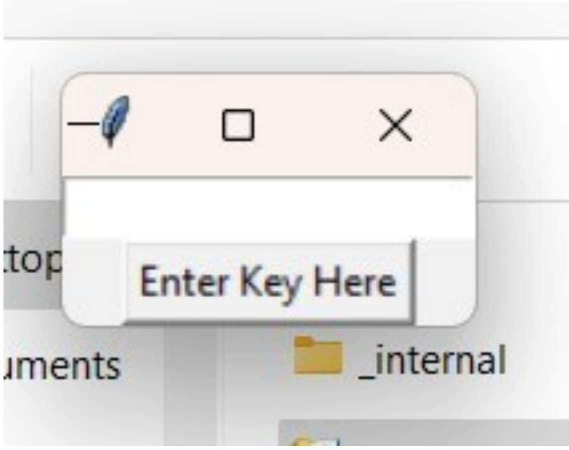
Ln 1, Col 1 | 24 characters | 100% | Windows (CRLF) | UTF-16 LE

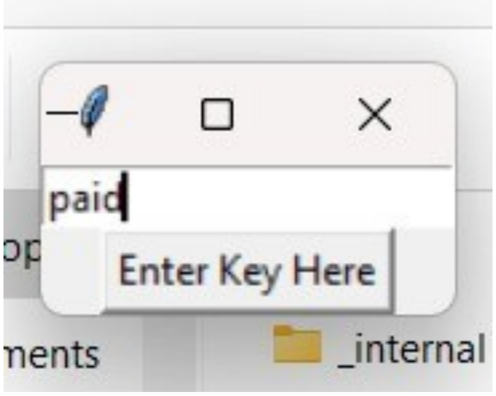
The Text File after decryption :-



```
Please Nawraz We want to Graduate
```

The client will write the input paid to receive key to decrypt files.





paid