

IS ASSIGNMENT 1

Wahaj Javed Alam – (20K-0208)

Implementation of AES:

AES-128:

```
PS D:\AES> python -u "d:\AES\20k-0208_AES.py"
[+] AES encryption
[+] Made by Wahaj Javed (20K-0208)
[+] Enter plaintext: You leave, you are no longer a part of this. You become a zero. If you stay, if you want to change the world, you become a yes. You become a one.
[+] Enter Key Size (128, 192, 256): 128
[+] Encrypting...
[+] Hex Representation of Plain Text: 596f75206c656176652c20796f7520617265206e6f206c6f6e67657220612070617274206f6620746869732e20596f75206265636f6d652061207a65726f2e20461792c20696620796f752077616e7420746f206368616e67652074686520776f726c642c20796f75206265636f6d652061207965732e20596f75206265636f6d652061206f6e652e
[+] Hex Representation of Key: fb946959d74d7bee41a84f81c9fa110e
[+] Number of Blocks: 10
[+] Number of Round Keys: 44
[+] Cipher Text: 47929bd588678e5660f57152ea078788995c5ba36be02d98cc8f00b3004c7843d58bbfa329bec2f8c5be3301af898c55f66d69b538360c7f2dc65a3fca202759c56c9a75935ee537384d3407f80d17bd72181e2d8ce3c6130730daed8620947e0020234aad245513b8235a4dc0146bf4c25709812eb956e2b8c54fd1f913230bada23d0f53fbc4f4ff32cbbb2f95872c2fa32fc58eb4a164a
[+] Decrypting...
[+] Number of Round Keys: 44
[+] Plaintext: You leave, you are no longer a part of this. You become a zero. If you stay, if you want to change the world, you become a yes. You become a one.
PS D:\AES>
```

AES-192:

```
PS D:\AES> python -u "d:\AES\20k-0208_AES.py"
[+] AES encryption
[+] Made by Wahaj Javed (20K-0208)
[+] Enter plaintext: You leave, you are no longer a part of this. You become a zero. If you stay, if you want to change the world, you become a yes. You become a one.
[+] Enter Key Size (128, 192, 256): 192
[+] Encrypting...
[+] Hex Representation of Plain Text: 596f75206c656176652c20796f7520617265206e6f206c6f6e67657220612070617274206f6620746869732e20596f75206265636f6d652061207a65726f2e20461792c20696620796f752077616e7420746f206368616e67652074686520776f726c642c20796f75206265636f6d652061207965732e20596f75206265636f6d652061206f6e652e
[+] Hex Representation of Key: 16067a313adf2c66a01d2ef6dda621fbbd78ebd744a4eaf2
[+] Number of Blocks: 10
[+] Number of Round Keys: 52
[+] Cipher Text: 4939d67cde6d194c5e07244f7b0e8ed6a46e117350423ac7513bd369afeaed9821071e951d82538e3300f8736ce885958499ed872d4a529170b56a68de5964c2ebc666801bdc3edd8bc79feb070c0889d09dec b848a11fe9df3a6d05c3519c2513ba19ee23856c2bdf89836c386fa1a4451c36d05250ae425d5699b8bfa8edf8d5dc2715200977a17634a83e333cc1c26d2c0e52ecdbe1c98358527252533c7
[+] Decrypting...
[+] Number of Round Keys: 52
[+] Plaintext: You leave, you are no longer a part of this. You become a zero. If you stay, if you want to change the world, you become a yes. You become a one.
PS D:\AES>
```

AES-256:

```
[+] Plaintext: You leave, you are no longer a part of this. You become a zero. If you stay, if you want to change the world, you become a yes. You become a one.
PS D:\AES> python -u "d:\AES\20k-0208_AES.py"
• [+] AES encryption
[+] Made by Wahaj Javed (20K-0208)
[+] Enter plaintext: You leave, you are no longer a part of this. You become a zero. If you stay, if you want to change the world, you become a yes. You become a one.
[+] Enter Key Size (128, 192, 256): 256
[+] Encrypting...
[+] Hex Representation of Plain Text: 596f75206c656176652c20796f7520617265206e6f206c6f6e67657220612070617274206f6620746869732e20596f75206265636f6d652061207a65726f2e20496620796f7520737461792c20696620796f752077616e7420746f206368616e67652074686520776f726c642c20796f75206265636f6d65206120796f732e20596f75206265636f6d652061206f6e652e
[+] Hex Representation of Key: fa69cb5ed4fe67838cfc0680381785bce1422e5d4bca65ee336e4887ac7329b4
[+] Number of Blocks: 10
[+] Number of Round Keys: 60
[+] Cipher Text: 291631213fac9d3705fdac54aef2733821ab67dcc599046a046beaec87911d6671dacfdabda76af067052102db03fd276e2aa94f86c5b860caa65c5338a2c656c37a61882be6e5dfc6eb535ccfbae4b60ef940ec2323f9c40131c5ec2b95577d885a1b5c46b3f1a614556b316c5fcb816e8ede3e60510ad029ac99b8248ed8920dfc57f1c5360391dc608af2868f3a8610c27f0d44f8fe88fa2fa7e59f93c9
[+] Decrypting...
[+] Number of Round Keys: 60
[+] Plaintext: You leave, you are no longer a part of this. You become a zero. If you stay, if you want to change the world, you become a yes. You become a one.
○ PS D:\AES> █
```