CSE4057 Information Systems Security

Homework 1 Report

Ahmet Onat Özalan - 150118054

Erdem Pehlivanlar - 150119639

1) Generation of public-private key pairs

1.a) RSA key pair (Key A)

```
Key A private:
308202750201003000D06092A864886F70D0101010500048202 5F3082025B02010002818100C2843904C13594
0B42AC83749BAF9E0BB3AB8157C34D8EA85DCD17D350F5F874EEF6E9220EFA43A76C35F5C6EEFCD8D26DB544
6F40C10A8E1004E61AD7C5EC37DF6E851B46737122349BA24FC49AB5A59D699BB8EDEF79D8F3BDC1D33D4305
28B57CAE71C01DBC4C1AE40173EEDF844648804E200468E1645EC17D8891F8E343020301000102818 00EC61F
7FE148E228AF74B8E5F76E86F0D941A7D39EF82F6351A9E28060AAD351D655EC991DF81B815B87B1AB881003
A135474A4904EB0F3E8105A39085B3A3B5976F26E7A7721D78764B1EF390DCA0F2E879E01603E44E3513E3EF
56D8F22D7D8564F08BDD4CBD856A6ADC901BB97A6803DF883914C92DA99E7A6336328DF0D9024100D863206B
F3C926785E917CDB67EA4CC2DF4D1CDC37C324FD871B1BFBA69E4E5D79F2DD39171ADD69D76455CFDC05FB83
D294D8EF048A38402A72FE0EE07DCD6D024100E62022E629CA5A93B2FC6B4B895654EBA7036B9DAD53F1C442
41B0E4C1C64673DC02797540984CE24D15ACC1BBDA17DCF782FB5FD135AC830CF66A300A72756F02405FFDF1
771249CCA01F4BA938E7EB5FAC1F456525283390A84B943220BBF4844D217924BC5BCC96268ADFBED59C04A7
63FE39FBD6648C3091FE82CEC3A8C1062D0240372824B53DF6FE56C063B7E3D6FB1647953440AAFE4C4C7A59
D71CEAF776EA94027BA558F12E8FDEFDD2E0215F411ACF1F94096421E4D78061AEFE2C9D9469890240760F51
2960583003C159C28703207AA0F16ED238EF58350DC6DF483835EEFE38672F3787DD49020E626EC570A031E6
E0C77066AD7DD5BAEF1C3662C9C39C0E56

Key A public:
30819F300D06092A864886F70D010101050003818D0030818902818100C2843904C135940B42AC83749BAF9E
0BB3AB8157C34D8EA85DCD17D350F5F874EEF6E9220EFA43A76C35F5C6EEFCD8D26DB5446F40C10A8E1004E6
1AD7C5EC37DF6E851B46737122349BA24FC49AB5A59D699BB8EDEF79D8F3BDC1D33D430528B57CAE71C01DBC
4C1AE40173EEDF844648804E200468E1645EC17D8891F8E3430203010001
```

1.b) Two ECDH key pairs (Key B and Key C)

```
Key B private:
3041020100301306072A8648CE3D020106082A8648CE3D030107042730250201010420F30B435783D6779513
E3301CB09E2BE5EA079A39804BC19E9AF6691369BC5B0A

Key B public:
3059301306072A8648CE3D020106082A8648CE3D030107034200 04E3154595E1F4AA28E4AD2117C889E21E46
E41B4194D73763E5BF2F103B353C146B4A4A612E6482463664BBAD5E9932F00D6FA126F78D56B45A16775F5A
F43E1D

Key C private:
3041020100301306072A8648CE3D020106082A8648CE3D030107042730250201010420AEE4368922681C3EF9
086038B43BC56CC77A87919B332AADBEF4E123D0E202B1

Key C public:
3059301306072A8648CE3D020106082A8648CE3D030107034200 04CD2BCA840E0033E51481B440E8BCF9D9E8
3CF27DCEFA3752457BC9ACEBE0B232CB9B3BA2E7656A3555B68AE8D3CE02E06AAE06C70180BCEABFA0B98A0E
FD1323
```

2) Generation of symmetric keys

2.a) Symmetric keys Key 1 and Key 2, their encrypted and decrypted values by Key A

```
Key 1:
EE8E7396FF68177A8BDD742FE445B426

Key 2:
18110B623DC0488DFADA27717B5DFE96AC3BA276C87D1D998C8723C9F62AFAF0

Key 1 encrypted with Key A public:
18EF3A4E5768C14FA46F21F1DB158D27803957FA10AB7EF7A42011D6C9C8C076970037B771F9B98E40DE8A00
6AE0C843FCCAF9D9ACB7C25EFA65EE4F280C0D73EDF89F7D87C516A26C9C87537E436146FC2E700A443B7B7A
30B84F2DB50093DDE89AFEB0BBE54DAA34A777DAE44F53D663852C820F002E8EB2DC44CAF22BDEB5

Key 2 encrypted with Key A public:
71C931209319F75860AF0D89B42DF6BB34A5521752093694A416B9321B005F4540444C16AD30E95309D9C263
CA9AD82B6F40CF6FA4C60AC97D6289482BD35456D67AD3BCA9B8BE2556EF4D11532ABFAE3BA0CC3295EF0D8B
39D79395DD4AD3F40008BDBE54395D7D2A2B88FB9C04AADD31CFDD92120480407E50EEAE7F21175A

Key 1 decrypted:
EE8E7396FF68177A8BDD742FE445B426

Key 2 decrypted:
18110B623DC0488DFADA27717B5DFE96AC3BA276C87D1D998C8723C9F62AFAF0
```

2.b) Symmetric key generation using ECDH key pairs Key B and Key C

```
Key generated using key-B-private and key-C-public:
97F7AD260A86F2A83F920A77D85EAE88F1F68218235D16FE2F51BCF3C12C7A40

Key generated using key-C-private and key-B-public:
97F7AD260A86F2A83F920A77D85EAE88F1F68218235D16FE2F51BCF3C12C7A40
```

3) Generation and verification of digital signature

```
Message digest H(m):
CA97497B626DA0065573E266E3607E51A4F391AAE088AFEB6B78A1FF2E6AF239

Digital signature:
3943A6B6582A5BFD6D649E07BA320E42A513FA68E51A39B84595AEF7441559F5BE3292F30F10C55CDF139AB3
551972D8845961CE005B8C46E945E14CF35C61C16B230FBC42B11CC65C27470515FE433461FF88CBCC963787
7794A1F29465BF79569BD2C0B41097A9EB0F0020D7C99C633482927FABD7AA02FC8A1A66D7DA5150

Digital signature decrypted with RSA public key:
CA97497B626DA0065573E266E3607E51A4F391AAE088AFEB6B78A1FF2E6AF239
```

4) AES encryption

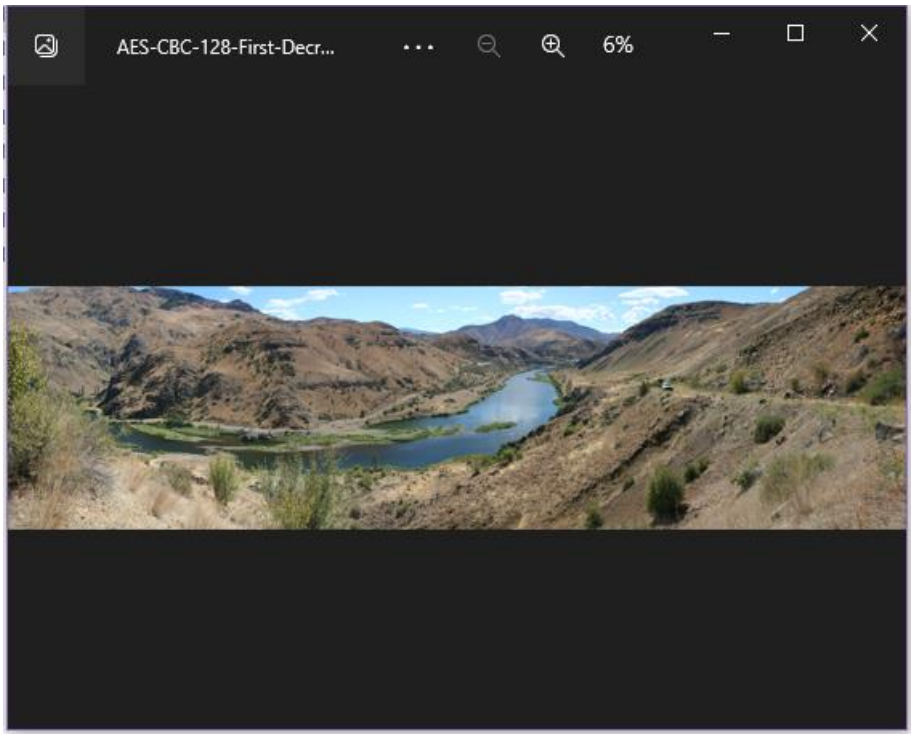
Encrypted files are in the “output” directory.

4.1) AES in CBC mode, 128-bit key

4.1.a) IV and the screenshot of the encrypted file

```
IV for AES in CBC mode, 128 bit key, first iteration:
6C5938233FC2D9BDAA9EBBDE06FE152E
```

4.1.b) Ciphertext decryption



4.1.c) Time elapsed for encryption

Comments are at the end of Section 4.

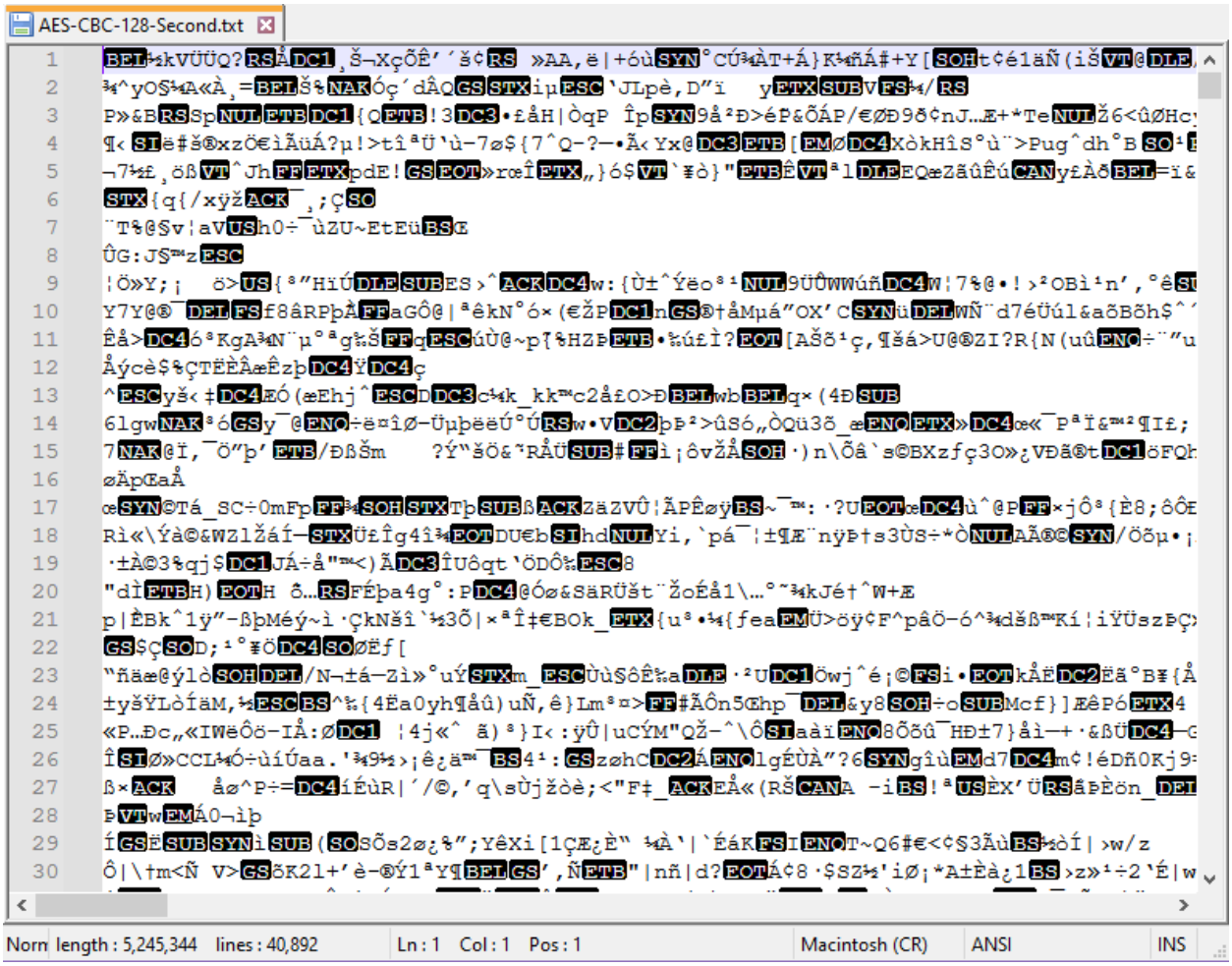
```
Time elapsed for encryption for AES in CBC mode, 128 bit key, first iteration:
41 ms
```

4.1.d) Comparison of ciphertexts from two different IVs

Second IV:

```
IV for AES in CBC mode, 128 bit key, second iteration:
D5AF2C4D9EBF57ED87448B68DC17EDA2
```

Second ciphertext: (next page)

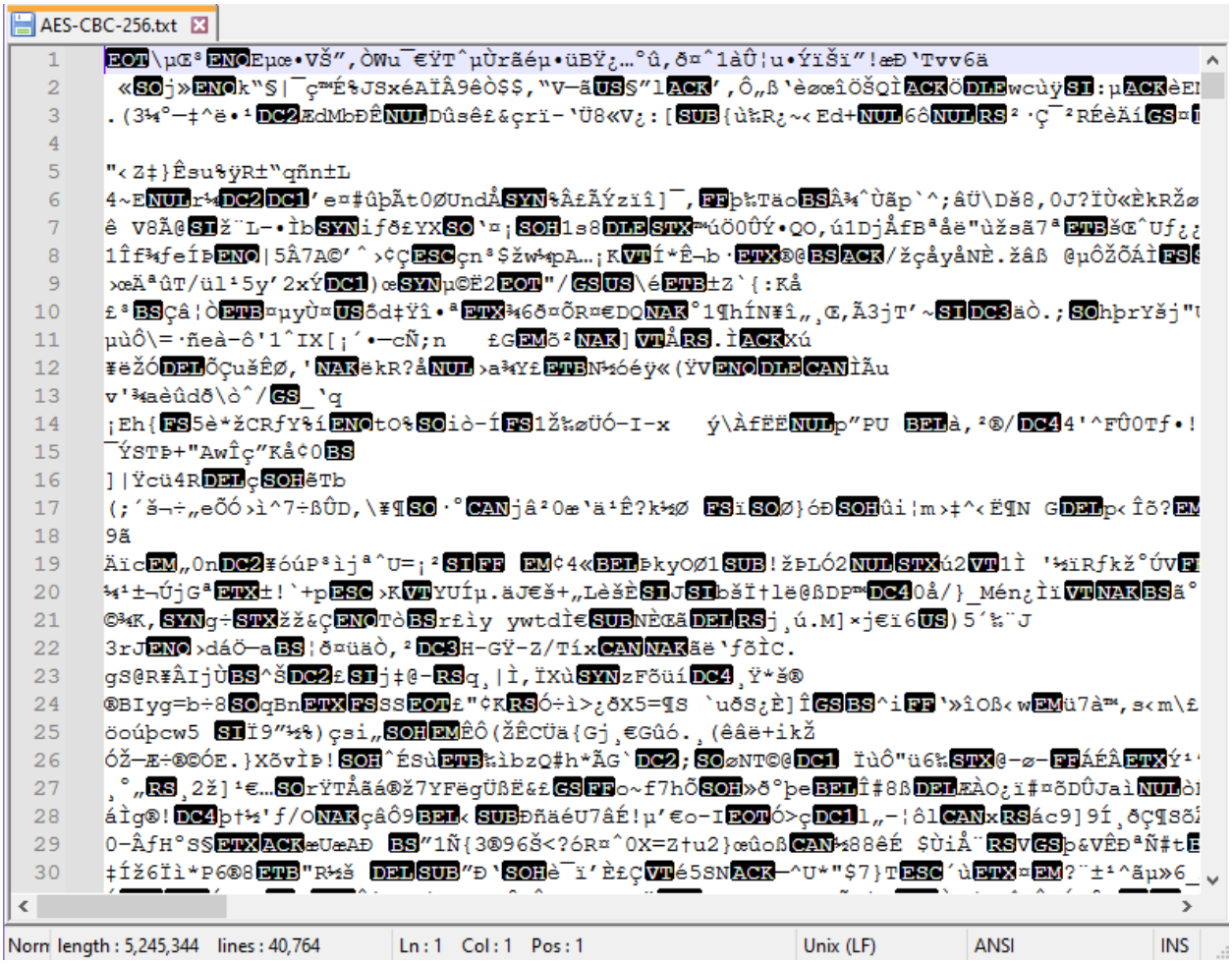


As it can be seen, this ciphertext is different from the one in 4.1.a.

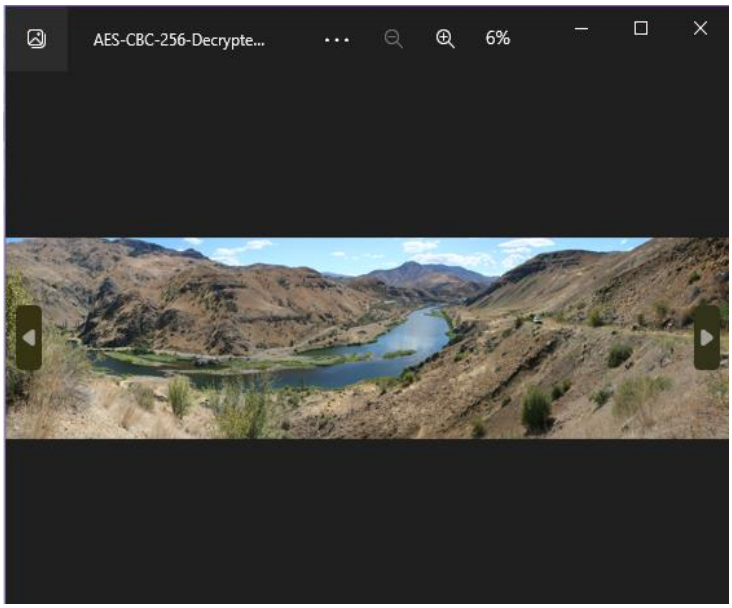
4.2) AES in CBC mode, 256-bit key

4.2.a) IV and the screenshot of the encrypted file

```
IV for AES in CBC mode, 256 bit key:
78558A3B9C7104670001722A6676C850
```



4.2.b) Ciphertext decryption



4.2.c) Time elapsed for encryption

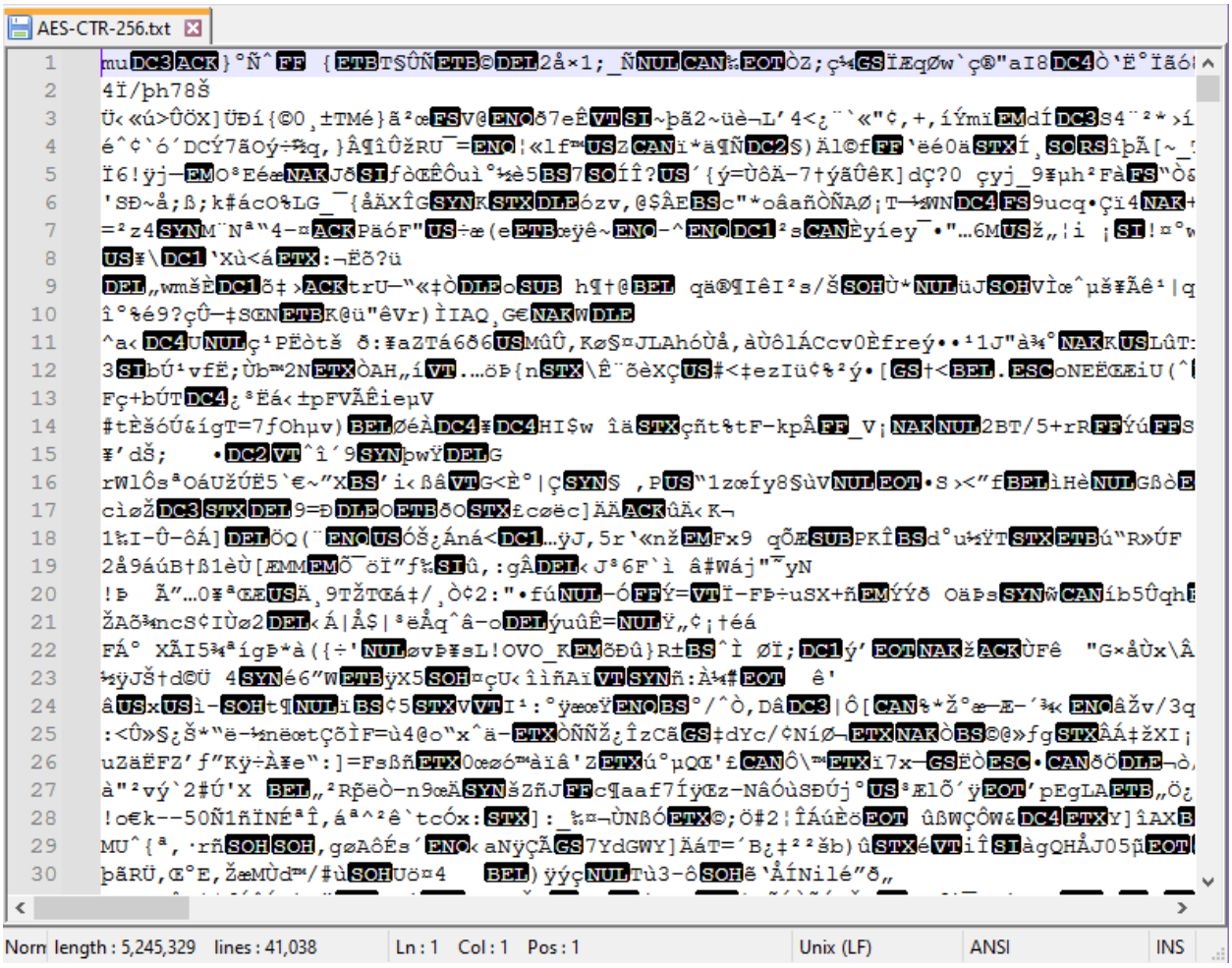
```
Time elapsed for encryption for AES in CBC mode, 256 bit key:
20 ms
```

4.3) AES in CTR mode, 256-bit key

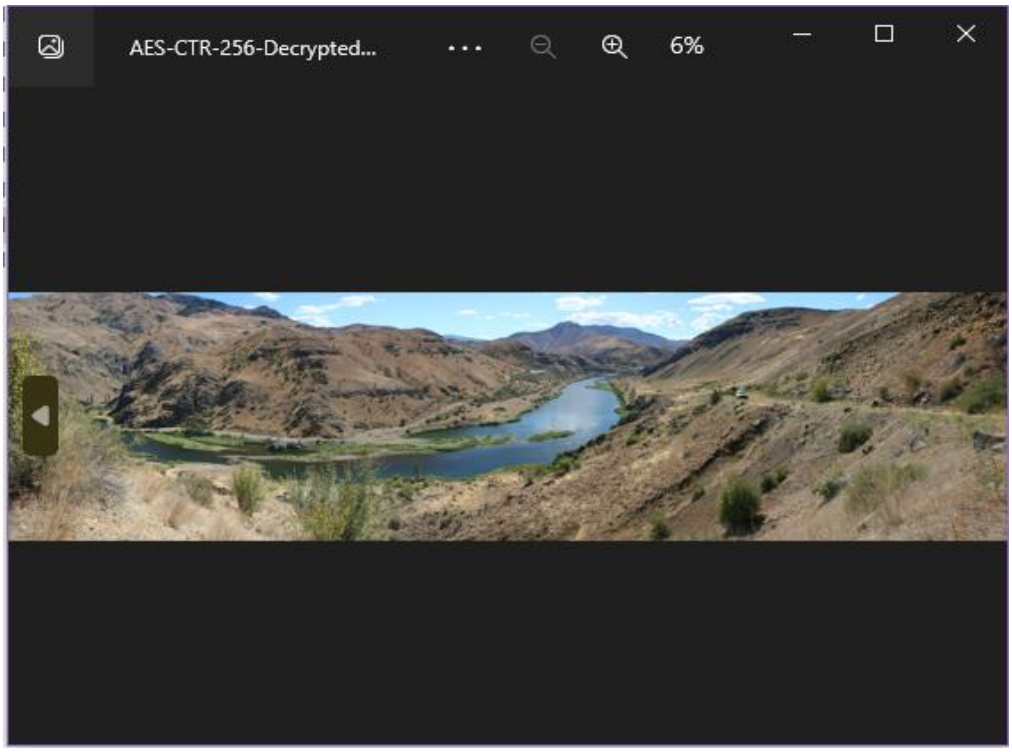
4.3.a) IV and the screenshot of the encrypted file

First 64 bits are the nonce, last 64 bits are the counter.

```
IV for AES in CTR mode, 256 bit key (Nonce is the first 64 bits):
30A265A87C0D83BC0000000000000000
```



4.3.b) Ciphertext decryption



4.3.c) Time elapsed for encryption

```
Time elapsed for encryption for AES in CTR mode, 256 bit key:
23 ms
```

4.4) Comments on elapsed times

Time elapsed for AES in:

- CBC mode, 128-bit key, first iteration: 41ms
- CBC mode, 128-bit key, second iteration: 25ms
- CBC mode, 256-bit key: 20ms
- CTR mode, 256-bit key: 23ms

Time elapsed for the first iteration of the CBC mode with 128-bit key is significantly higher than the other elapsed times. I believe this is not related to the algorithms themselves but related to our software execution environment (IDE etc.).

Other elapsed times show no significant difference between them.

5) Message authentication code of a text message

Text message is in the “myText.txt” file.

```
MAC of the text message:
12CD0155E2F3B0E32AB71A8A11006B1A38D6851F9686CD36F30B7FBE7AFC3CFB

New key generated by applying HMAC-256 to K2:
6411249E4EC799B761CCCD464AC4BF3E57EA677B5C43C583F54EA18FEE820F47
```