

# 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:

30820275020100300D06092A864886F70D01010105000482025F3082025B02010002818100C2843904C13594  
0B42AC83749BAF9E08B3AB8157C34D8EA85DCD17D350F5F874EEF6E9220EFA43A76C35F5C6EEFCD8D26DB544  
6F40C10A8E1004E61AD7C5EC37DF6E851B46737122349BA24FC49AB5A59D699B88EDEF79D8F3BDC1D33D4305  
28B57CAE71C01DBC4C1AE40173EEDF844648804E200468E1645EC17D8891F8E34302030100010281800EC61F  
7FE148E228AF7488E5F76E86F0D941A7D39EF82F6351A9E28060AAD351D655EC991DF81B815887B1AB881003  
A135474A4904EB0F3E8105A39085B3A3B5976F26E7A7721D78764B1EF390DCA0F2E879E01603E44E3513E3EF  
56D8F22D7D8564F08BDD4C8D856A6ADC901BB97A6803DF883914C92DA99E7A6336328DF0D9024100D863206B  
F3C926785E917CD867EA4CC2DF4D1CDC37C324FD871B18FBA69E4E5D79F2DD39171ADD69D76455CFDC05F8B3  
D294D8EF048A38402A72FE0EE07DCD6D024100E62022E629CA5A93B2FC6B48895654EBA7036B9DAD53F1C442  
41B0E4C1C64673DC02797540984CE24D15ACC18BDA17DCF782FB5FD135AC830CF66A300A72756F02405FFDF1  
771249CCA01F4BA938E7EB5FAC1F456525283390A84B9432208BF4844D217924BC5BCC96268ADF8ED59C04A7  
63FE39FBD6648C3091FE82CEC3A8C1062D0240372824B53DF6FE56C063B7E3D6FB1647953440AAFE4C4C7A59  
D71CEAF776EA94027BA558F12E8FDEFDD2E0215F411ACF1F94096421E4D78061AEFE2C9D9469890240760F51  
2960583003C159C28703207AA0F16ED238EF58350DC6DF483835EEFE38672F3787DD49020E626EC570A031E6  
E0C77066AD7DD5BAEF1C3662C9C39C0E56

Key A public:

30819F300D06092A864886F70D010101050003818D0030818902818100C2843904C135940B42AC83749BAF9E  
08B3AB8157C34D8EA85DCD17D350F5F874EEF6E9220EFA43A76C35F5C6EEFCD8D26DB5446F40C10A8E1004E6  
1AD7C5EC37DF6E851B46737122349BA24FC49AB5A59D699B88EDEF79D8F3BDC1D33D430528B57CAE71C01DBC  
4C1AE40173EEDF844648804E200468E1645EC17D8891F8E3430203010001

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

Key B private:

3041020100301306072A8648CE3D020106082A8648CE3D030107042730250201010420F30B435783D6779513  
E3301C809E2BE5EA079A39804BC19E9AF6691369BC5B0A

Key B public:

3059301306072A8648CE3D020106082A8648CE3D03010703420004E3154595E1F4AA28E4AD2117C889E21E46  
E41B4194D73763E5BF2F103B353C146B4A4A612E6482463664BBAD5E9932F00D6FA126F78D56B45A16775F5A  
F43E1D

Key C private:

3041020100301306072A8648CE3D020106082A8648CE3D030107042730250201010420AEE4368922681C3EF9  
086038B43BC56CC77A87919B332AADBEF4E123D0E202B1

Key C public:

3059301306072A8648CE3D020106082A8648CE3D03010703420004CD2BCA840E0033E51481B440E8BCF9D9E8  
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:

3943A6B6582A5BFD6D649E07BA320E42A513FA68E51A39884595AEF7441559F5BE3292F30F10C55CDF139AB3  
551972D8845961CE005B8C46E945E14CF35C61C16B230FBC42B11CC65C27470515FE433461FF88CBCC963787  
7794A1F29465BF79569BD2C0B41097A9EB0F0020D7C99C633482927FABD7AA02FC8A1A66D7DA5150

Digital signature decrypted with RSA public key:

CA97497B626DA0065573E266E3607E51A4F391AAE088AFEB6B78A1FF2E6AF239

Encrypted files are in the “output” directory.

#### 4.1) AES in CBC mode, 128-bit key

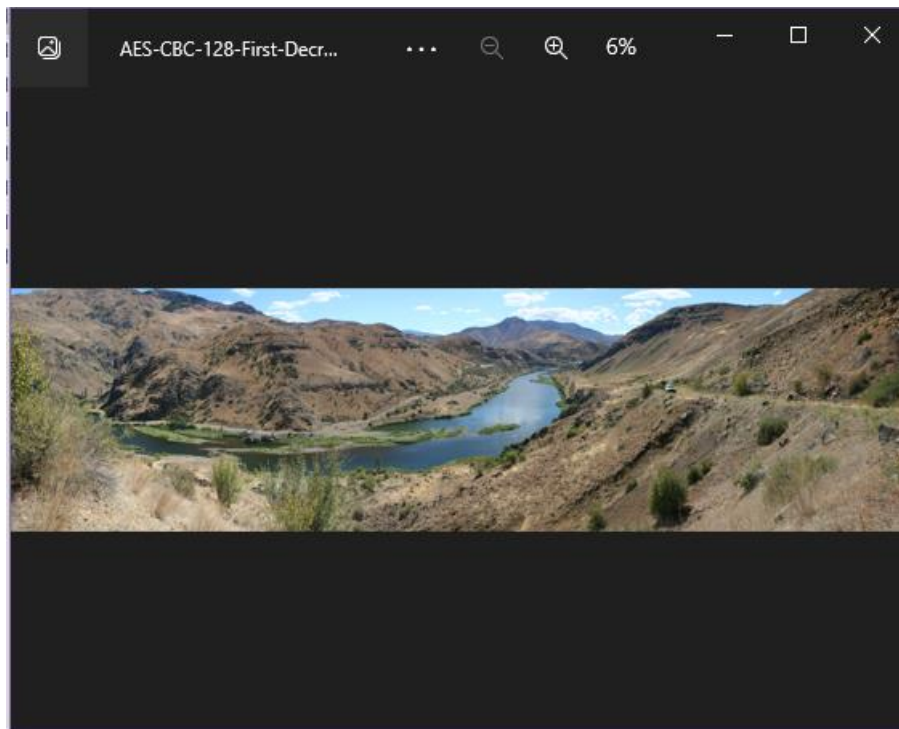
#### 4.1.a) IV and the screenshot of the encrypted file

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

6C5938233FC2D9BDAA9EBBDE06FE152E

```
AES-CBC-128-First.txt x
1 "æÐàDLE·Zñî^h.VT^ÜGj-ESCpIX>y{·ÅÄÄ9Ší(¯q°0Á¾ÜfaÄiDC3ÉÐ\FðØRSŽ·H°iôÔéFRS·Ñ-BS^
2 æ=fèù†j·h·^óACKæÖ°-Igdè²°PGSKâBETM-stHACKiî÷;FRÅWH}NAR+ô-ÓN*/1GS(SOH)\Ebóbkê,
3 \?WÆ-@SI°·ù|ETXàcS\VTî†iLDC4âpfX,®W\IcP.pùC¾,jíHë#ç²,ÿæ"ÄdiUS«E°(
4 [ÿTDWG;kt·æE=„V9i*,°;sDLET?GY°ESch...i ÅÄŽ^IH_nBS" _NáBELETXó-FSÐSOO#°Ü)RSðEOTÑ...
5 @^>÷UøðÄDC2j
6 v'Ž×"1DC1°SO(STXðûwBETBÉi9RSYðE²;MD6)×4-ENOŽDLETFF>J|ô+šÆJ;RESC7US|+ñÉRS°«6^
7 æ6Äñ|@-°ùæGS@%|CANg÷iSTX\ð³fÜðèÿhDC1q1@/QðaU7 ENOFÄ-Ê# Ý!@S«...DC1»ðÓ|+g·|¾^v#«
8 cDLE^a^°% »USEOTNULÖÄ°SùNULèø;ô¿Š°#STXKC=æSIðSOH×IM-ÄiÄ <Bì-ÄcUS²NUL²«ESCÉi< >
9 °i¾RS00USæiFðDC3z°Öumð,fETXñETX°¢÷+Š† QáÄ}Äp,VTDLEÉq|°...<ACK°mF°DLEÜÜDC4ET
10 Eyw·ÆŽž|ä×DC2iäšh4|Äæ5áíL^ä°GSHi95°8[°z@Äè...Pð08SOH4DC1è4D°RBþZ vXNAK,,@ècBS9
11 ð7¾N<ä|[Fq?>MDÉLOFS×,žðÍí°^CANÖÄ°Wá<;RHACKç99EOT°JGhî>DLEÄSUB)ÿ(®¾÷Ä¾6|af)°:
12 fè Ü-DC1ká-fçÜä,×Nvác9vÜ°A!iðÑETB|fSYN°æK1ñi°pT°°SYNf#3i°EðRS°zçUSè,Üxv4çGÜ(Ä
13 ÈUSfc,NAKETX-p¾ðÖ°-æç;¾²CK2N²;{.EM²²°iÄP^BEL2SIUa¾GSi,µ F[É6äÜJ?lÜÑ†-#@uNULñ÷i
14 ÄBLg±
15 <NðÉFä ððóZ:9ESC>âDEL
16 Ü->çýNULÄj·2èððÄÜKCAN°J°EMÜDLESSÈ -°×gN;ñSšáíLÄÜîÐÜj6ñÁEðEOTüÖ°÷ùBELštçææE
17 ASYNBELFSäSiÄANULDC1i81ç·WçETBUwaÄGyFÄ°0zSUBDVtE2STXxð°QWÜ°FWv^°fó{YÄ¾æ5CrÄ
18 Jç÷[...]|DC3R Üf(STXKBELBD°,è,ÄSO+Yr¾VqçFSE<¾CANzeÜ²æ°xEM°p÷ÈcKäçNAK :È[¾NAKbiACKi
19 DC2ÄDLEBSCBSEY°iG2pçžqññ<ä.bDC1@°ESC
20 æÄ+çÿ DC3KšpN, BELiðóS<†:|q €NAKšdACKqfzè8#GS7<ähÿu°ááé[_gig#;s&°QðÄEQè×KtM
21 ð°5fa5D°hETBi;üü°»ævQ8pðEžšQBSFYH^@ETXSrEM°ÄEó?Èpi!@SIy@7ižDLEB5ýNULš;¾
22 ^ið>f°xi&ÜLð°A°-|ðSgú OCAN6ER]ß_ð8-jBSÄß†iLÖ:ÚoGS×«k
23 ÜDC4g¾¾;¹-ÜÈ¾
24 ²çX¾qUSß-FSið-ETXið
25 \¾ñM„b„-Äbo|¾S...š¾¾Lið°tä7çæäñX{äñÈè<äSACKðFFçVTðÜè\ççp?žž>SßDC2DC22?ÿSI 07×SOH
26 <ðä¾,µaè¿°R3FSð°µEMC÷óð_ ;|Oçff/t^,gÄðÿè>sSOHHe+@YÄrUSð0Èæ _j-FSj@|/ÿÄÄÜXRSY2
27 °mÄ:
28 »5i°j-u-è-·SYNyýDC2Jqó÷+G×ETXý²>ÿEn¾6ä°üÜEÄðSiSOjRSESC>÷çW<pf ð-è&È°Ä;ä|;
29 ETX/BçP(¿.µ°á°ó+°æÜ\NäDLENULðEYBEL·ðNAK°°)=ENOBS†è(6Ä†šðxçs_SO>s_tøiîjfaä(1Ü
30 tuqßÄSYNyçESCrbEüiç4è>..K<).ACK0°è°ÜKSTX6ðè°i[°ÄAETXÁiB<DC3,áo°æWÄTPNððf,iðüw
```

#### 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)

```
AES-CBC-128-Second.txt
1 BEL*kvUÜQ?RSÄDC1,š-XçÖÊ' 'šçRS »AA,è|+óùSYN°CÚ*ÀT+Á}K*ñÁ#+Y[SOHtçé1aÑ(išVT@DLE.
2 3^yOS*4A«À,=BELš%NARóç'dAQGSSTXipESC`JLpè,D"i yETXSUBVFS4/RS
3 P»&BRSspNULETBDC1{QETB!3DC3.éÅH|òqP ÎpSYN9â²D>éP&ÖÁP/€Ø9ðçnJ...Æ+*TeNULž6<ûØHç:
4 q<SIè#š@xzöëiÄuÄ?u!>tîªü`ù-7ø$ {7^Q-?-•Ä<Yx@DC3ETB[EMØDC4XòkHîS°ù">Pug^dh°B SO:
5 -7*Æ,òßVT`JhFEETXpdE!GSËOT»rœîETX,,}ó$VT`æð)"ETBÊVTª1DLEEQæZâûÊúCANYéÄöBEL=i&
6 STX{q{/xyžACK_,;çSO
7 "T%$Sv|avUSH0÷-ùZU~EtEuBSË
8 ŪG:JS"zESC
9 !Ö>Y;| ø>US{°"HiÚDLESUBES>^ACKDC4w:{Ü±^Ýeoª¹NUL9ÜÜWWúñDC4W!7%•!>²OBì¹n',°éSI
10 Y7Y@Ø DELFSF8ÂRPbÄFFagô@|ªékN°ó×(€žPDC1nGS@+âMpá"OX'C SYNüDELWN`d7éÜú1&aðBðhS^`
11 Êâ>DC4óªKgA³N"µ°ªg%šFFqESCúÜè~p{HHzETB.ªú£î?EOT[ASð¹ç,qšá>U@ZI?R{N(uüENO÷""u
12 Áýcèš%çTEÊÄæÊzþDC4YDC4ç
13 ^ESCyš<þDC4Æó(æEhj^ESCDDC3c4k_kk"²2â£O>ðBELwbBELq×(4ðSUB
14 6lgwNAKªóGSy`@ENO÷èªið-ÜpþèèÜ°ÚRSw•VDC2p²²>ûsó,,ÖQü3ð æENOETX»DC4æ«Pªi£ª²qI£;
15 7NAK@î,`ö"p'ETB/ðBšm ?Ý"šöæ²RÄÜSUB#FFî,ðvžÅSOH·)n\ðâ`s@BXzfç3O>çVðä@tDC1óFQk
16 øÄpEaÄ
17 æSYN@Tá_SC÷0mFpFFªSOHSTXTpSUBßACKZäZVÜ!ÄPêøýBS~"ª:·?UEOTæDC4ù@PFF×jÔª{È8;ðÖE
18 Ri«\Ýa@æWZ1žáí-STXÜèîg4iªPOTDUEbSIhdNULYi,`pá`!±qÆ"nyþts3ÜS÷*ÖNULÄ@çSYN/Öðµ.¡
19 ·±À@3%çj$DC1JÁ÷ª""<)ÄDC3îUðqt`ÖDó%ESCð
20 "diETBH)EOTH ð...RSFÉpa4g°:PDC4@óæ&SâRÜšt`žöÉâ1\...ªkJé+^W+Æ
21 p|ÈBk^1ý"-ßpMéý~ì·çkNšî`ª3Ö|ªªîþEBOK_ETX{uªª{feaEMÜ>öýçF^pâÖ-óªdšßªKí;iiYÜszþç;
22 GSççSOD;ªªçDC4SOðE£[
23 "ñææýlðSOHDEL/N-±á-Zi»°uÝSTXm ESCÜùSðÊªaDLEª²UDC1Öwj^é;@FSi•POTkÅÊDC2Eä°Bª{Å
24 ±yšYLöIam,ªESCBSªª{4Ea0yhqáú)uN,è)LmªªFF#ÄÖn5Ghp DEL&y8SOH÷oSUBMcf}]ÆèPóETX4
25 «P...ðc,,«IWèÖð-IÄ:ØDC1 14j«^ ä)ª}I<:ýÜ|uCYM"Qž-^`ðSIaàîENO8Öðú`Hð±7}âi-+·æBÜDC4-C
26 îSIØ»CClªó÷ùîUaa.'ª9ª>|éçªªBS4¹:GSzøhçDC2ÄENOlgÉÜÀ"?6SYNgîùEMd7DC4mç!éDñ0Kj9:
27 B×ACK Åø^P÷=DC4iÉùR|`/®,`q\ªÜjžðè;<"FþACKEÄ«(RšCANA -iBS!ªUSEX`ÜRSâþÈön_DEI
28 BVTwEMÄ0-îþ
29 íGSËSUBSYNîSUB(SOSðs2øçª";YéXi[1çÆçÈ"ªÀ`|`ÉÁKFSIENOT~Q6#€<ç$3ÄùBSªðí|>w/z
30 Ô|tmcÑ V>GSðK2l+`è-@Ý1ªYqBELGS',NËETB"|nñ|d?EOTÁç8·$SZª¹ið;ªA±èäç1BS>zªª÷²É|w
```

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

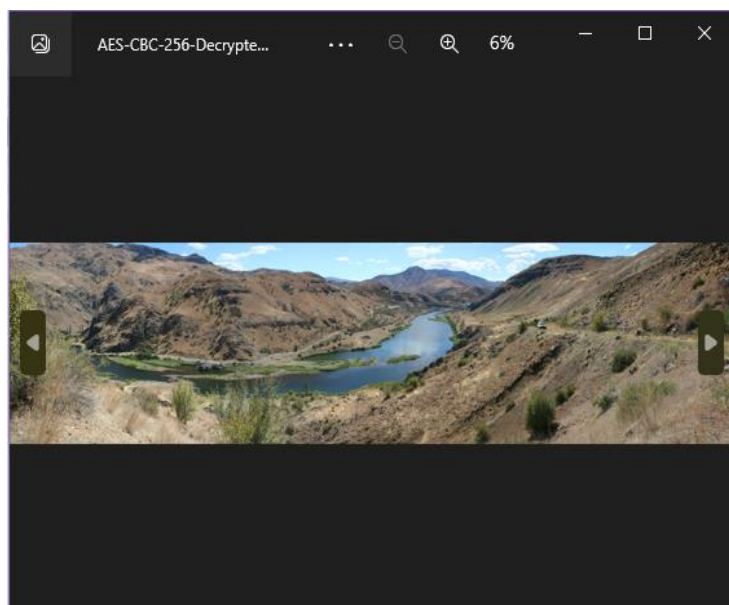
IV for AES in CBC mode, 256 bit key:

78558A3B9C7104670001722A6676C850



```
AES-CBC-256.txt
1  EOT\µG°ENOEmce•VŠ",òWu_€YT^µÙrãép•ùBYç...°û,ð^1àÛ!u•ÝiŠi"!æÐ'Tvv6ä
2  «SOj»ENOk"S|_ç™É%JSxéAïÄ9èò$S,"v-äUSS"lACK',Ô,,ß`èzœiôŠQlACKÖDLEwcùÿSI:µACKèEi
3  .(3¼°-†^è•¹DC2EdMbðÊNULDûsêé&çri-`Ü8«Vç:[SUB{ù%Rç~<Ed+NUL6ôNULRS²·Ç²RéèÄiGS=I
4
5  "<Z†}Êsu%ÿR±"qñntL
6  4~ENULr*DC2DC1'e#ûpÄt0ØUndÄSYN*ÄzÄÝziij],FFp%TaoBSÄ*^Üäp`^;äÜ\Dš8,0J?iÜ«ÈkRŽø
7  ê v8Ä@SIž`L-•İbSYNifðzYXSO"q;SOHls8DLESTX™ú00ÛÝ•QO,ú1DjÄfB*âe"ùzsä7ªETBšG^Ufçç
8  1îf*feifBENO|5Ä7A@'^>çÇESCçn*Šžw*pa...;KVTİ*Ê-b·ETX@BSACK/žçâyâNÈ.žâß @µôžÖÄiFSè
9  »œÄ*ût/ùl¹5y'2xÝDC1)œSYNµ@Ê2EOT"/GSUS/éETB±z`{:Kâ
10 zªBSÇâ;òETB=µyÛ=USðd†Ýi•ªETX*6ð=ðR=EQNAK¹1qHİN#i,,G,Ä3jT'~SIDC3aò.;SOHprYšj"t
11 µùò\=·ñeà-ð¹¹IX[;'-cN;n    £GEMð²NAK]VTÄRS.İACKKú
12  #èžÖDELÔçušÊØ,'NAKèkR?âNUL>a*YiETBN*óéÿ«(ÿVENODLECANiÄu
13  v'ªaeûdð\ð^/GS_`q
14  ;Eh{FS5è*žCRfY%İENOtO%SOİð-fFS1ž%šÜÓ-I-x    ý\ÀfÈENULp"PU BELà,²@/DC44'^FÜ0Tf•!
15  _ÝSTB+"Awİç"Kâç0BS
16  ]|ÿcù4RDELçSOHšTb
17  (;'š÷÷,œçÖ>î^7÷ßÜD,\#qSO•°CANjâ²0æ¹a¹Ê?k*Ø  FSiSOØ}óðSOHûi!m;†^<ÈqN GDELp<İð?EM
18  9ä
19  ÄicEM,,OnDC2#óÚP*İjª^U=;²SIFF EMç4«BELBkyOØ1SUB!žBLÓ2NULSTXú2VT1İ 'ªİrfkž°ÚVFI
20  ¼¹±-ÚjGªETX±!'+pESC>KVTYUİp.äJ€š+„LešÈSTJbšİ†le@ßDF™DC40â/)_MénçİiVTNAKBSä°
21  @ªK,SYNG=STXžž&çENOTòBSrily ywtđieSUBNÈGâDELRSj,ú.M)×j€İ6US)5'‰"J
22  3rJENO>dáÖ-aBS!ð=uaò,²DC3H-GÝ-Z/TixCANNAKæ'fðİc.
23  gs@R#ÄIjùBS^šDC2E SIj†@-RSq,İ,İxùSYNZFöüiDC4,Ý*š@
24  @BIyq=b÷8SOqBnETXFSSSFOT£"çKRSó÷ì>ç8X5=qS `uðSçÈ]İGSBS^İFF`»iOß<wEMü7à™,s<m\£
25  ðoùpcw5 SIİ9"¼)çsi,,SOHEMEÔ(žÈCŪa{Gj,€Gûó.,(èâe+ikž
26  Óž-E÷@çOE.}Xðvİß!SOH^ÉSùETB%ibzQ#h*ÄG`DC2;SOøNT@çDC1 İùÔ"ù6%STX@-ø-FFÁÉÂETXÝ¹
27  ,°„RS,2ž]¹€...SORÿTÄÄä@ž7YfegÜßÈ&£GSFFo~f7hðSOH»ð°peBELİ#8ßDELEAO;İ#ðDÜJaiNULòl
28  áİg@!DC4pt*¼f/ONAKçâô9BEL<SUBðñäéU7âÉ!µ'€o-İEOTó>çDC1l,,-;ðlCAN×RSác9]9İ,ðçqSðİ
29  0-ÄfH°SSETXACK=UæAD BS¹1N{3@96š<?ðR=^0X=Ztu2)œûoßCAN*88éÉ SÜiÄ`RSVGSjpaVÊðªN#tE
30  †İž6İi¹P6@8ETB"R*š DELSUB"ð`SOHè¹i'È£çVTé5SNACK-^U*"S7}TESC'ùETX=EM?`±¹^äµ»6_
```

#### 4.2.b) Ciphertext decryption

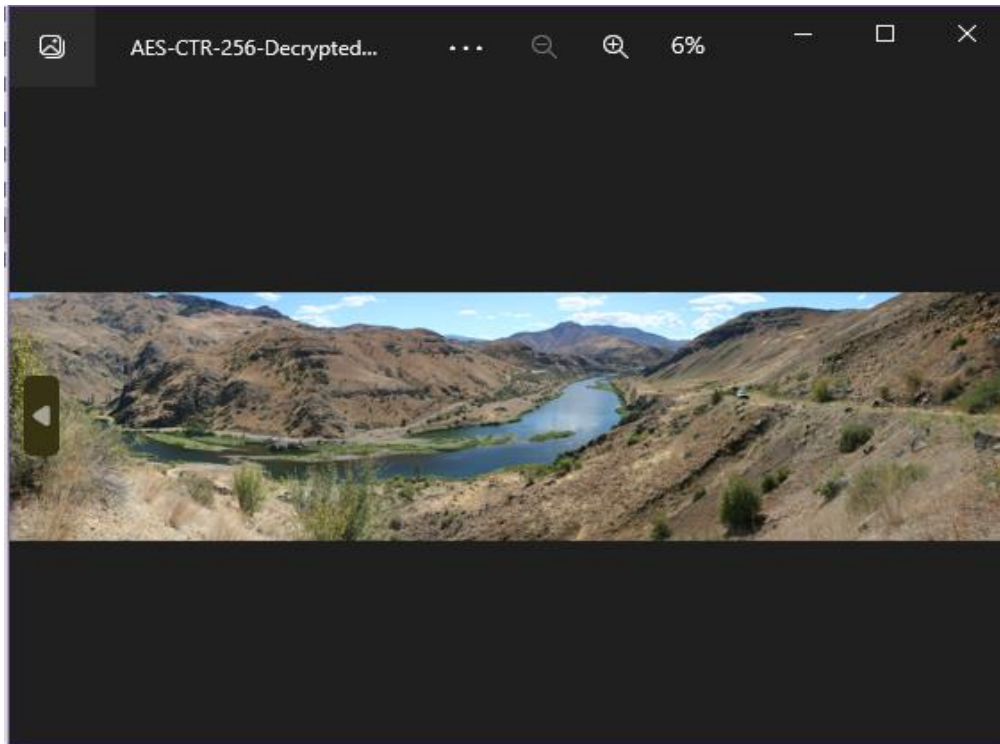


```

1 muDC3ACK}°Ñ^FF {ETBTSÛÑETB@DEL2â*1;_ÑNULCAN:EOTÔZ;ç;GSİEzQw`ç@°aİ8DC40`È°İäö!^
2 4i/ph78š
3 Ü<«ú>ÜÖX}Üİ1{[0,±TMé}ä²αFSV6ENQđ7eÊVTSI~pâ2~üè-L'4<;`«`ç,+,íymİEMdíDC3S4`²*²>İ
4 é<ç`ó`DCY7aOý÷q,}ÄqİÜžRU=ENQ!<lF™US2CANİ*²aİÑDC2S)Äl@fFF`eé0aSTXİf,İORSİpÄ[~.
5 İ6!ýj~EMO°EeēNAKJ8SİfđGEôuİ°²e5BS7SOİf?US'}ý=Üä8-7+yäÜëK}dç?0 çyj_9şph²FâFS`Ôs
6 'SD~â;ß;k#âcO°LG_ {äÄXİGSYNRSTXDLEózv,çŞAEBSç"°oâñðÑAØ;T~WNDC4FS9ucq.Çİ4NAK+
7 =²z4SYNM`N²"4~=ACKPaöF"US÷æ(eETBşýê~ENQ~^ENQDC1²sCANËyİey~"...6MUSž,,İ;SI!²°w
8 US#\\DC1'Xù<áETX:-Èö?ü
9 DEL,,wmšÈDC1šç>ACKtrU~«çòDLEcSUB hq+@BEL qä@QİêI²s/šSOHÜ* NULüJSOHVİø^pšŞÄê¹|q
10 İ°²é9?çÜ~÷SCENETBK@ü"èVr) İIAQ,GEÑAKWDLE
11 ^a.DC4UNULç¹PEðtš 8:ŞazTá6š6USMûÜ,KøŞ=JLAhøÜä,äÜšlÁCCv0Èfreý..¹J"à²°NAKRUSLût:
12 3SİbÜ¹vfÊ;Üb=2NETXÒAH,,İVT...øP{nSTXİÊ`ðèXçUS#<hezİüç²ý.[GS+<BEL.ESCøNEÈGEİU(^
13 Fç+bÚTDC4ç²ŠâktpFVÄİepV
14 #tÈšöÜ&İGT=7fOhuv)BELØéÄDC4ŞDC4Hİšw İäSTXçñtçtF-kpÂFF_V;NAKNUL2BT/5+rRFFYúFES
15 Ş'dš; •DC2VT`İ¹9SYNpwYDELG
16 rWlôš°OáuZÜÈ5`è~XBS'İkßÄVTG<È`|çSYNS ,PUS`l²æİy8SùVNUL:EOT•S>~fBELİHèNULGSðE
17 cİøžDC3STXDEL9=ðDLBcETBđOSTXİcøēç|ÄÄACKÜÄ<K~
18 lKİ-Ü-ðÄ}DELÖQ(`ENQUSÖš;Änä<DC1...yJ,5r`«nžEMFx9 qÖESUBPKİßBSd°u²YtSTXETBú"R»ÜF
19 2Ä9äÜB+ßlèÜ[EMMEMÖ öİ"fçSİÜ,,gÄDELJ²6F`İ äŞWáj"™YN
20 !P Ä"...0°²çEUSA,9TžTGEä÷,Öç2:"•fúNUL-óFFY=VTİ-FP=usX+ñEMYÝŠ OäPŞSYNWCANİb5Üqhİ
21 ŽÄ³ncsçİÜø2DEL<Á|ÄS|²eÄq`ä-cDELýuüÈ=NULY,,ç;téä
22 FÁ° XÄİ5²²İgP²ª({÷'NULøvpPŞsL!OVO KEMšDÜ)R±BS`İ Øİ;DC1ý'EOTNAKžACKÜFè "G×âùx\Ä
23 ²yJŠ±dCÜ 4SYNé6"WEtBYX5SOH=çU<İñAiVTSYNñ:Ä²#EOT è'
24 äUSUSİ-ŠOHTçNULİBSç5STXVVTİ:²:ýæYENQBS°/°ò,DäDC3|Ø[CAN²²ž°E~E~²K ENQÖäžv/3q
25 <Ü>çSİž°²E~İnèctçİF=Ü4çO"x²a-ETXÖNNž;İzCäGS±dYç/çNİØ-ETXNAKòBS@çfgSTXÄÄžžXI|
26 uzaÈFZ'f"Ky÷ÄŞe":}=FßñETXOøøó²äİ¹ZETXú°µQEİ²CANò\™ETXİ7x-GSÈòESC.CANšöDLE-ò,
27 à"²vY²#Ü'X BEL,,²Rpeò-n9æASYNšžRİFFçİaaf7İyEz-NáòùSDÜj°US²Eİö'ýEOT'pEgLAETB,,òç
28 !øKk-50NİñİNEÄİ,ä²²è²'tcÓx:STX]:Ş=ÜNßÓETX;Ø#2;İÄüÈšEOT ÜBWCÖW&DC4ETXYİAXE
29 MU`{²,·rñSOHŠOH,gøAöÉš'ENQ°anYçÄGS7YdGWYİÄT=²Bç²²šb)ÜSTXèVTİİSİägQHÄJ05pEOT
30 pÄRÜ,ç°E,žæMÜD™/ŞÜSOHÜø=4 BEL)ýçNULtù3-šSOHŞ'Äİnİlè"š,,

```

#### 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