Network and Telecommunications Systems Security

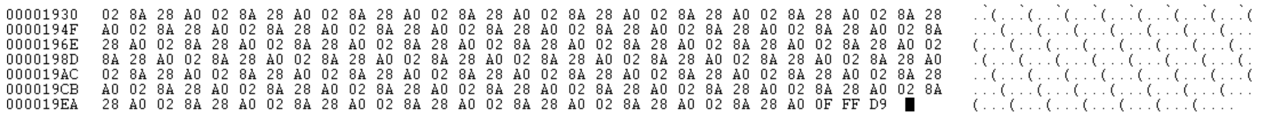
Homework_2

AM: EN2190001

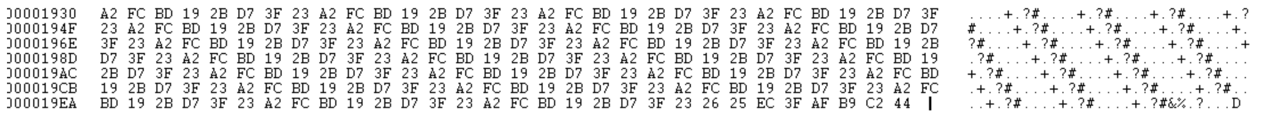
Name :Evangelos Siatiras

Exercise_1_A

In Electronic Code Book (ECB) mode of operation does not require IV for encryption as the input plain text will be divided into blocks and each block will be encrypted with the key provided and hence identical plain text blocks are encrypted into identical cipher text blocks. Obviously, by scrolling to end in the original and encrypted image in hex we realize that the structure in the ciphertext is identical and only the ascii values have changed.



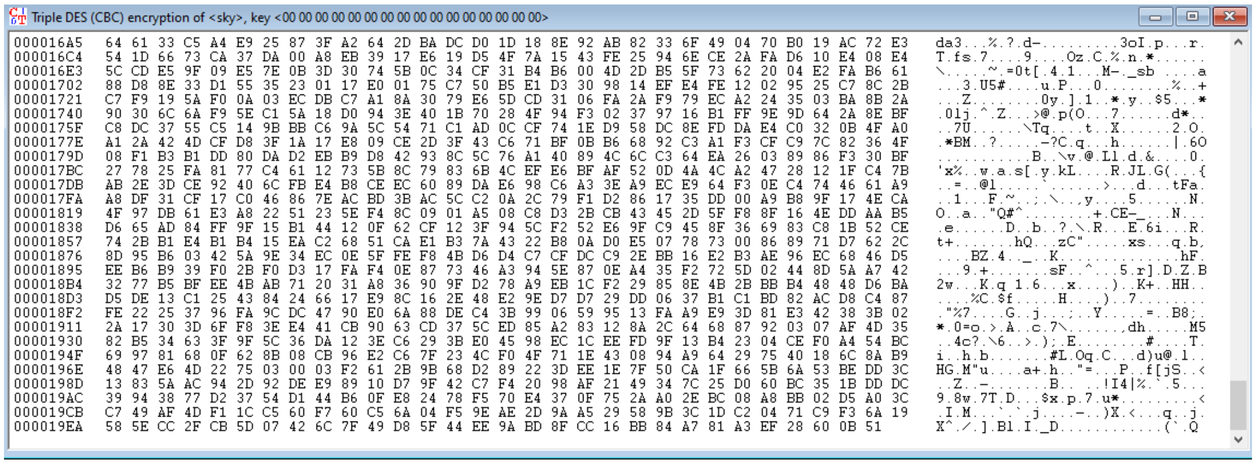
```
00001930   02 8A 28 A0 02 8A 28 A0 02 8A 28 A0 02 8A 28 A0 02 8A 28 A0 02 8A 28 A0 02 8A 28 A0 02 8A 28   .`(..`(..`(..`(..`(..`(..`(..`(
0000194F   A0 02 8A 28 A0 02 8A 28 A0 02 8A 28 A0 02 8A 28 A0 02 8A 28 A0 02 8A 28 A0 02 8A 28 A0 02 8A   ...(...(...(...(...(...(...(...
0000196E   28 A0 02 8A 28 A0 02 8A 28 A0 02 8A 28 A0 02 8A 28 A0 02 8A 28 A0 02 8A 28 A0 02 8A 28 A0 02   (...(...(...(...(...(...(...(..
0000198D   8A 28 A0 02 8A 28 A0 02 8A 28 A0 02 8A 28 A0 02 8A 28 A0 02 8A 28 A0 02 8A 28 A0 02 8A 28 A0   .(...(...(...(...(...(...(...(.
000019AC   02 8A 28 A0 02 8A 28 A0 02 8A 28 A0 02 8A 28 A0 02 8A 28 A0 02 8A 28 A0 02 8A 28 A0 02 8A 28   ..(...(...(...(...(...(...(...(
000019CB   A0 02 8A 28 A0 02 8A 28 A0 02 8A 28 A0 02 8A 28 A0 02 8A 28 A0 02 8A 28 A0 02 8A 28 A0 02 8A   ...(...(...(...(...(...(...(...
000019EA   28 A0 02 8A 28 A0 02 8A 28 A0 02 8A 28 A0 02 8A 28 A0 02 8A 28 A0 02 8A 28 A0 0F FF D9         (...(...(...(...(...(...(....
```



```
00001930   A2 FC BD 19 2B D7 3F 23 A2 FC BD 19 2B D7 3F 23 A2 FC BD 19 2B D7 3F 23 A2 FC BD 19 2B D7 3F   ....+.?#....+.?#....+.?#....+.?
0000194F   23 A2 FC BD 19 2B D7 3F 23 A2 FC BD 19 2B D7 3F 23 A2 FC BD 19 2B D7 3F 23 A2 FC BD 19 2B D7   #....+.?#....+.?#....+.?#....+.
0000196E   3F 23 A2 FC BD 19 2B D7 3F 23 A2 FC BD 19 2B D7 3F 23 A2 FC BD 19 2B D7 3F 23 A2 FC BD 19 2B   ?#....+.?#....+.?#....+.?#....+
0000198D   D7 3F 23 A2 FC BD 19 2B D7 3F 23 A2 FC BD 19 2B D7 3F 23 A2 FC BD 19 2B D7 3F 23 A2 FC BD 19   .?#....+.?#....+.?#....+.?#....
000019AC   2B D7 3F 23 A2 FC BD 19 2B D7 3F 23 A2 FC BD 19 2B D7 3F 23 A2 FC BD 19 2B D7 3F 23 A2 FC BD   +.?#....+.?#....+.?#....+.?#...
000019CB   19 2B D7 3F 23 A2 FC BD 19 2B D7 3F 23 A2 FC BD 19 2B D7 3F 23 A2 FC BD 19 2B D7 3F 23 A2 FC   .+.?#....+.?#....+.?#....+.?#..
000019EA   BD 19 2B D7 3F 23 A2 FC BD 19 2B D7 3F 23 A2 FC BD 19 2B D7 3F 23 26 25 EC 3F AF B9 C2 44      ..+.?#....+.?#....+.?#&%.?...D
```

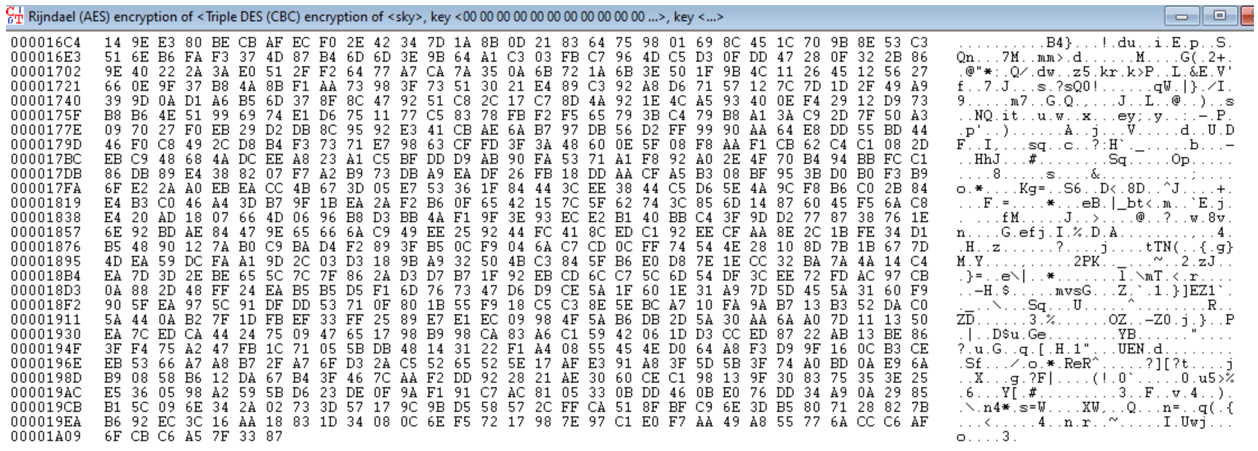
Exercise_1_B

In the cipher block chaining (CBC) mode of operation, an initialization vector (IV) is exclusive-ored with the plaintext prior to encryption. For the first round of encryption, this is a random, public value. For subsequent rounds, it is the ciphertext of the previous round. This is intended to fix the issue with ECB mode where identical plaintext blocks create identical ciphertext blocks. In case that there is no IV we have always the same output for a message so an attacker can guess changed blocks. Among the differences between AES and 3DES like the encryption key length and block length by using the same mode of operation CBC in our case ensures that in every round of the encryption the ciphertext is "combined" with the ciphertext in the previous round (at first with IV) so the structure of the ciphertext in both cases will be different. Of course, there are differences in the structure of the ciphertext resulted from AES and 3DES because the encryption is totally different as mentioned above.



Triple DES (CBC) encryption of <sky>, key <00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>

```
000016A5   64 61 33 C5 A4 E9 25 87 3F A2 64 2D BA DC D0 1D 18 8E 92 AB 82 33 6F 49 04 70 B0 19 AC 72 E3   da3...%.?.d-.........3oI.p...r.
000016C4   54 1D 66 73 CA 37 DA 00 A8 EB 39 17 E6 19 D5 4F 7A 15 43 FE 25 94 6E CE 2A FA D6 10 E4 08 E4   T.fs.7....9....Oz.C.%.n.*......
000016E3   5C CD E5 9F 09 E5 7E 0B 3D 30 74 5B 0C 34 CF 31 B4 B6 00 4D 2D B5 5F 73 62 20 04 E2 FA B6 61   \.....~.=0t[.4.1...M-._sb ....a
00001702   88 D8 8E 33 D1 55 35 23 01 17 E0 01 75 C7 50 B5 E1 D3 30 98 14 EF E4 FE 12 02 95 25 C7 8C 2B   ...3.U5#....u.P...0........%..+
00001721   C7 F9 19 5A F0 0A 03 EC DB C7 A1 8A 30 79 E6 5D CD 31 06 FA 2A F9 79 EC A2 24 35 03 BA 8B 2A   ...Z........0y.].1..*.y..$5...*
00001740   90 30 6C 6A F9 5E C1 5A 18 D0 94 3E 40 1B 70 28 4F 94 F3 02 37 97 16 B1 FF 9E 9D 64 2A 8E BF   .0lj.^.Z...>@.p(O...7......d*..
0000175F   C8 DC 37 55 C5 14 9B BB C6 9A 5C 54 71 C1 AD 0C CF 74 1E D9 58 DC 8E FD DA E4 C0 32 0B 4F A0   ..7U......\Tq....t..X......2.O.
0000177E   A1 2A 42 4D CF D8 3F 1A 17 E8 09 CE 2D 3F 43 C6 71 BF 0B B6 68 92 C3 A1 F3 CF C9 7C 82 36 4F   .*BM..?.....-?C.q...h......|.6O
0000179D   08 F1 B3 B1 DD 80 DA D2 EB B9 D8 42 93 8C 5C 76 A1 40 89 4C 6C C3 64 EA 26 03 89 86 F3 30 BF   ...........B..\v.@.Ll.d.&....0.
000017BC   27 78 25 FA 81 77 C4 61 12 73 5B 8C 79 83 6B 4C EF E6 BF AF 52 0D 4A 4C A2 47 28 12 1F C4 7B   'x%..w.a.s[.y.kL....R.JL.G(...{
000017DB   AB 2E 3D CE 92 40 6C FB E4 B8 CE EC 60 89 DA E6 98 C6 A3 3E A9 EC E9 64 F3 0E C4 74 46 61 A9   ..=..@l.....`......>...d...tFa.
000017FA   A8 DF 31 CF 17 C0 46 86 7E AC BD 3B AC 5C C2 0A 2C 79 F1 D2 86 17 35 DD 00 A9 B8 9F 17 4E CA   ..1...F.~..;.\..,y....5......N.
00001819   4F 97 DB 61 E3 A8 22 51 23 5E F4 8C 09 01 A5 08 C8 D3 2B CB 43 45 2D 5F F8 8F 16 4E DD AA B5   O..a.."Q#^........+.CE-_...N...
00001838   D6 65 AD 84 FF 9F 15 B1 44 12 0F 62 CF 12 3F 94 5C F2 52 E6 9F C9 45 8F 36 69 83 C8 1B 52 CE   .e......D..b..?.\.R...E.6i...R.
00001857   74 2B B1 E4 B1 B4 15 EA C2 68 51 CA E1 B3 7A 43 22 B8 0A D0 E5 07 78 73 00 86 89 71 D7 62 2C   t+.......hQ...zC".....xs...q.b,
00001876   8D 95 B6 03 42 5A 9E 34 EC 0E 5F FE F8 4B D6 D4 C7 CF DC C9 2E BB 16 E2 B3 AE 96 EC 68 46 D5   ....BZ.4.._..K..............hF.
00001895   EE B6 B9 39 F0 2B F0 D3 17 FA F4 0E 87 73 46 A3 94 5E 87 0E A4 35 F2 72 5D 02 44 8D 5A A7 42   ...9.+.......sF..^...5.r].D.Z.B
000018B4   32 77 B5 BF EE 4B AB 71 20 31 A8 36 90 9F D2 78 A9 EB 1C F2 29 85 8E 4B 2B BB B4 48 48 D6 BA   2w...K.q 1.6...x....)..K+..HH..
000018D3   D5 DE 13 C1 25 43 84 24 66 17 E9 8C 16 2E 48 E2 9E D7 D7 29 DD 06 37 B1 C1 BD 82 AC D8 C4 87   ....%C.$f.....H....)..7........
000018F2   FE 22 25 37 96 FA 9C DC 47 90 E0 6A 88 DE C4 3B 99 06 59 95 13 FA A9 E9 3D 81 E3 42 38 3B 02   ."%7....G..j...;..Y.....=..B8;.
00001911   2A 17 30 3D 6F F8 3E E4 41 CB 90 63 CD 37 5C ED 85 A2 83 12 8A 2C 64 68 87 92 03 07 AF 4D 35   *.0=o.>.A..c.7\......,dh.....M5
00001930   82 B5 34 63 3F 9F 5C 36 DA 12 3E C6 29 3B E0 45 98 EC 1C EE FD 9F 13 B4 23 04 CE F0 A4 54 BC   ..4c?.\6..>.);.E........#....T.
0000194F   69 97 81 68 0F 62 8B 08 CB 96 E2 C6 7F 23 4C F0 4F 71 1E 43 08 94 A9 64 29 75 40 18 6C 8A B9   i..h.b.......#L.Oq.C...d)u@.l..
0000196E   48 47 E6 4D 22 75 03 00 03 F2 61 2B 9B 68 D2 89 22 3D EE 1E 7F 50 CA 1F 66 5B 6A 53 BE DD 3C   HG.M"u....a+.h.."=...P..f[jS..<
0000198D   13 83 5A AC 94 2D 92 DE E9 89 10 D7 9F 42 C7 F4 20 98 AF 21 49 34 7C 25 D0 60 BC 35 1B DD DC   ..Z..-.......B.. ..!I4|%.`.5...
000019AC   39 94 38 77 D2 37 54 D1 44 B6 0F E8 24 78 F5 70 E4 37 0F 75 2A A0 2E BC 08 A8 BB 02 D5 A0 3C   9.8w.7T.D...$x.p.7.u*.........<
000019CB   C7 49 AF 4D F1 1C C5 60 F7 60 C5 6A 04 F5 9E AE 2D 9A A5 29 58 9B 3C 1D C2 04 71 C9 F3 6A 19   .I.M...`.`.j....-..)X.<...q..j.
000019EA   58 5E CC 2F CB 5D 07 42 6C 7F 49 D8 5F 44 EE 9A BD 8F CC 16 BB 84 A7 81 A3 EF 28 60 0B 51      X^./.].Bl.I._D...........(`.Q
```

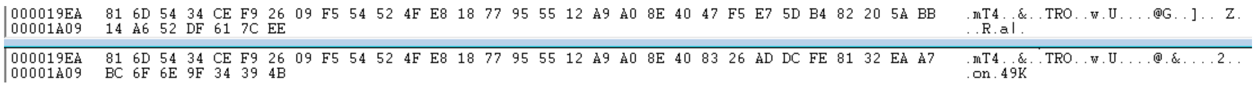


Rijndael (AES) encryption of <Triple DES (CBC) encryption of <sky>, key <00 00 00 00 00 00 00 00 00 00 00 ...>, key <...>

```
000016C4   14 9E E3 80 BE CB AF EC F0 2E 42 34 7D 1A 8B 0D 21 83 64 75 98 01 69 8C 45 1C 70 9B 8E 53 C3   ..........B4}...!.du..i.E.p..S.
000016E3   51 6E B6 FA F3 37 4D 87 B4 6D 6D 3E 9B 64 A1 C3 03 FB C7 96 4D C5 D3 0F DD 47 28 0F 32 2B 86   Qn...7M..mm>.d......M....G(.2+.
00001702   9E 40 22 2A 3A E0 51 2F F2 64 77 A7 CA 7A 35 0A 6B 72 1A 6B 3E 50 1F 9B 4C 11 26 45 12 56 27   .@"*:.Q/.dw..z5.kr.k>P..L.&E.V'
00001721   66 0E 9F 37 B8 4A 8B F1 AA 73 98 3F 73 51 30 21 E4 89 C3 92 A8 D6 71 57 12 7C 7D 1D 2F 49 A9   f..7.J...s.?sQ0!......qW.|}./I.
00001740   39 9D 0A D1 A6 B5 6D 37 8F 8C 47 92 51 C8 2C 17 C7 8D 4A 92 1E 4C A5 93 40 0E F4 29 12 D9 73   9.....m7..G.Q.,...J..L..@..)..s
0000175F   B8 B6 4E 51 99 69 74 E1 D6 75 11 77 C5 83 78 FB F2 F5 65 79 3B C4 79 B8 A1 3A C9 2D 7F 50 A3   ..NQ.it..u.w..x...ey;.y..:.-.P.
0000177E   09 70 27 F0 EB 29 D2 DB 8C 95 92 E3 41 CB AE 6A B7 97 DB 56 D2 FF 99 90 AA 64 E8 DD 55 BD 44   .p'..).......A..j...V.....d..U.D
0000179D   46 F0 C8 49 2C D8 B4 F3 73 71 E7 98 63 CF FD 3F 3A 48 60 0E 5F 08 F8 AA F1 CB 62 C4 C1 08 2D   F..I,...sq..c..?:H`._......b...-
000017BC   EB C9 48 68 4A DC EE A8 23 A1 C5 BF DD D9 AB 90 FA 53 71 A1 F8 92 A0 2E 4F 70 B4 94 BB FC C1   ..HhJ...#.........Sq.....Op.....
000017DB   86 DB 89 E4 38 82 07 F7 A2 B9 73 DB A9 EA DF 26 FB 18 DD AA CF A5 B3 08 BF 95 3B D0 B0 F3 B9   ....8.....s....&..........;....
000017FA   6F E2 2A A0 EB EA CC 4B 67 3D 05 E7 53 36 1F 84 44 3C EE 38 44 C5 D6 5E 4A 9C F8 B6 C0 2B 84   o.*....Kg=..S6..D<.8D..^J....+.
00001819   E4 B3 C0 46 A4 3D B7 9F 1B EA 2A F2 B6 0F 65 42 15 7C 5F 62 74 3C 85 6D 14 87 60 45 F5 6A C8   ...F.=....*...eB.|_bt<.m..`E.j.
00001838   E4 20 AD 18 07 66 4D 06 96 B8 D3 BB 4A F1 9F 3E 93 EC E2 B1 40 BB C4 3F 9D D2 77 87 38 76 1E   . ...fM.....J..>....@..?..w.8v.
00001857   6E 92 BD AE 84 47 9E 65 66 6A C9 49 EE 25 92 44 FC 41 8C ED C1 92 EE CF AA 8E 2C 1B FE 34 D1   n....G.efj.I.%.D.A..........4.
00001876   B5 48 90 12 7A B0 C9 BA D4 F2 89 3F B5 0C F9 04 6A C7 CD 0C FF 74 54 4E 28 10 8D 7B 1B 67 7D   .H..z......?....j....tTN(..{.g}
00001895   4D EA 59 DC FA A1 9D 2C 03 D3 18 9B A9 32 50 4B C3 84 5F B6 E0 D8 7E 1E CC 32 BA 7A 4A 14 C4   M.Y....,.....2PK.._...~..2.zJ..
000018B4   EA 7D 3D 2E BE 65 5C 7C 7F 86 2A D3 D7 B7 1F 92 EB CD 6C C7 5C 6D 54 DF 3C EE 72 FD AC 97 CB   .}=..e\|..*.......l.\mT.<.r....
000018D3   0A 88 2D 48 FF 24 EA B5 B5 D5 F1 6D 76 73 47 D6 D9 CE 5A 1F 60 1E 31 A9 7D 5D 45 5A 31 60 F9   ..-H.$.....mvsG...Z.`.1.}]EZ1`.
000018F2   90 5F EA 97 5C 91 DF DD 53 71 0F 80 1B 55 F9 18 C5 C3 8E 5E BC A7 10 FA 9A B7 13 B3 52 DA C0   ._..\...Sq...U.....^........R..
00001911   5A 44 0A B2 7F 1D FB EF 33 FF 25 89 E7 E1 EC 09 98 4F 5A B6 DB 2D 5A 30 AA 6A A0 7D 11 13 50   ZD......3.%......OZ..-Z0.j.}..P
00001930   EA 7C ED CA 44 24 75 09 47 65 17 98 B9 98 CA 83 A6 C1 59 42 06 1D D3 CC ED 87 22 AB 13 BE 86   .|..D$u.Ge........YB......"....
0000194F   3F F4 75 A2 47 FB 1C 71 05 5B DB 48 14 31 22 F1 A4 08 55 45 4E D0 64 A8 F3 D9 9F 16 0C B3 CE   ?.u.G..q.[.H.1"...UEN.d........
0000196E   EB 53 66 A7 A8 B7 2F A7 6F D3 2A C5 52 65 52 5E 17 AF E3 91 A8 3F 5D 5B 3F 74 A0 BD 0A E9 6A   .Sf.../.o.*.ReR^.....?][?t....j
0000198D   B9 08 58 B6 12 DA 67 B4 3F 46 7C AA F2 DD 92 28 21 AE 30 60 CE C1 98 13 9F 30 83 75 35 3E 25   ..X...g.?F|....(!.0`.....0.u5>%
000019AC   E5 36 05 98 A2 59 5B D6 23 DE 0F 9A F1 91 C7 AC 81 05 33 0B DD 46 0B E0 76 DD 34 A9 0A 29 85   .6...Y[.#.........3..F..v.4..).
000019CB   B1 5C 09 6E 34 2A 02 73 3D 57 17 9C 9B D5 58 57 2C FF CA 51 8F BF C9 6E 3D B5 80 71 28 82 7B   .\.n4*.s=W....XW,..Q...n=..q(.{
000019EA   B6 92 EC 3C 16 AA 18 83 1D 34 08 0C 6E F5 72 17 98 7E 97 C1 E0 F7 AA 49 A8 55 77 6A CC C6 AF   ...<.....4..n.r..~.....I.Uwj...
00001A09   6F CB C6 A5 7F 33 87                                                                            o....3.
```

Exercise_1_2

By changing the last digit from D9 to D8 we get the following result.



```
000019EA   81 6D 54 34 CE F9 26 09 F5 54 52 4F E8 18 77 95 55 12 A9 A0 8E 40 47 F5 E7 5D B4 82 20 5A BB   .mT4..&..TRO..w.U....@G..].. Z.
00001A09   14 A6 52 DF 61 7C EE                                                                            ..R.al.
```

```
000019EA   81 6D 54 34 CE F9 26 09 F5 54 52 4F E8 18 77 95 55 12 A9 A0 8E 40 83 26 AD DC FE 81 32 EA A7   .mT4..&..TRO..w.U....@.&....2..
00001A09   BC 6F 6E 9F 34 39 4B                                                                            .on.49K
```

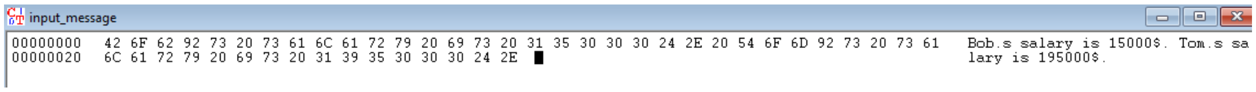
Obviously the values of the last block (last 128 bits so 16 bytes) in the above image is totally different.During the encryption process the plaintext is passed through 4 steps (SubBytes, ShiftRows, MixColumns, AddRoundKey) for many rounds.If we were able to find something in common AES would be a weak encryption algorithm based on alphabetic substitution.

Exersice_2_A

At first intuitively as the message consisting of 48 characters (48 bytes) and DES has message blocks of 64 bit (8 bytes) so the resulting ciphertext will consist of 6 blocks of 8 characters each.As the mode of operation is ECB means that the resulting ciphertext with the same key will always be the same. Thus we could start to guess the mapping of the plain text to cipher text was.So if we replace the blocks of 8 bytes containing the name Bob with the one containing the name Tom and vice versa we get the expected result.

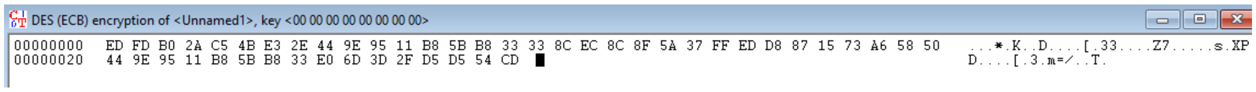
Proof:

We start with the initial Message



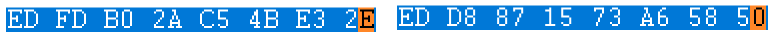
```
input_message
00000000   42 6F 62 92 73 20 73 61 6C 61 72 79 20 69 73 20 31 35 30 30 30 24 2E 20 54 6F 6D 92 73 20 73 61   Bob.s salary is 15000$. Tom.s sa
00000020   6C 61 72 79 20 69 73 20 31 39 35 30 30 30 24 2E                                                   lary is 195000$.
```

And we encrypt it using DES(ECB) with the key as per below in the image and we get :



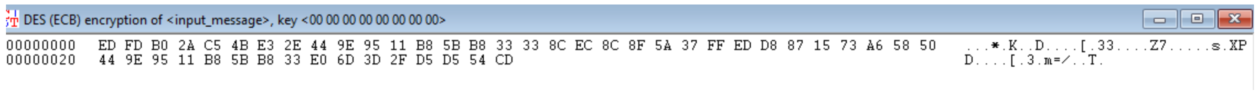
```
DES (ECB) encryption of <Unnamed1>, key <00 00 00 00 00 00 00 00>
00000000   ED FD B0 2A C5 4B E3 2E 44 9E 95 11 B8 5B B8 33 33 8C EC 8C 8F 5A 37 FF ED D8 87 15 73 A6 58 50   ...*.K..D....[.33....Z7.....s.XP
00000020   44 9E 95 11 B8 5B B8 33 E0 6D 3D 2F D5 D5 54 CD                                                   D....[.3.m=/..T.
```

Then the two concerning blocks are the ones below:



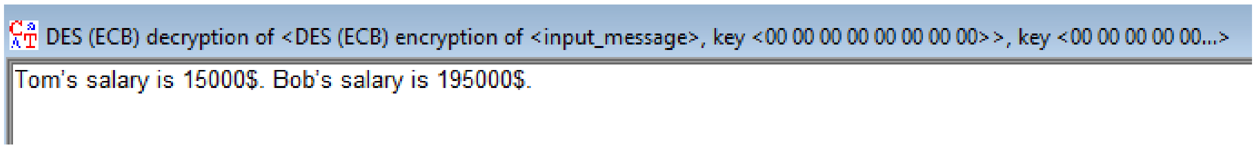
```
ED FD B0 2A C5 4B E3 2E  ED D8 87 15 73 A6 58 50
```

And by doing the necessary text replacements we get the following ciphertext:



```
DES (ECB) encryption of <input_message>, key <00 00 00 00 00 00 00 00>
00000000   ED FD B0 2A C5 4B E3 2E 44 9E 95 11 B8 5B B8 33 33 8C EC 8C 8F 5A 37 FF ED D8 87 15 73 A6 58 50   ...*.K..D....[.33....Z7.....s.XP
00000020   44 9E 95 11 B8 5B B8 33 E0 6D 3D 2F D5 D5 54 CD                                                   D....[.3.m=/..T.
```

And the decrypted message is :



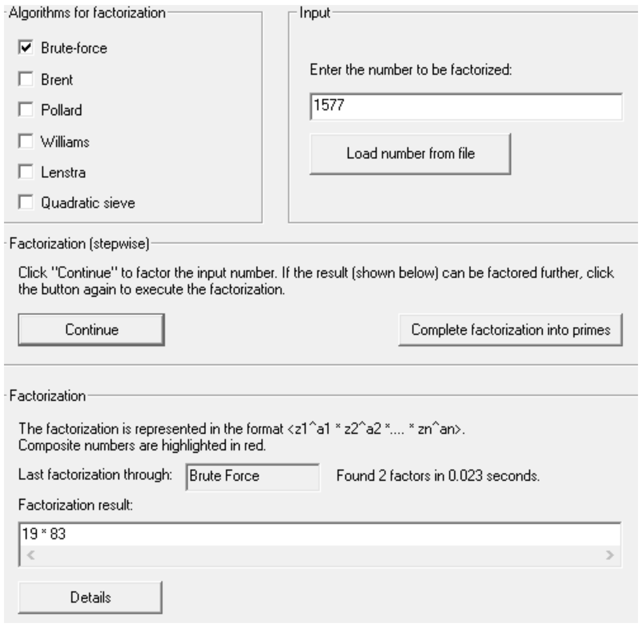
```
DES (ECB) decryption of <DES (ECB) encryption of <input_message>, key <00 00 00 00 00 00 00 00>>, key <00 00 00 00 00...>
Tom's salary is 15000$. Bob's salary is 195000$.
```

Exersice_2_B

If the original plaintext is smaller than the AES block size (128 bits regardless of the key size) so it fits into a single block then editing it in a meaningful way without knowing the key is not feasible yet and if it is done the AES encryption will be broken. Once the plaintext is longer than one block, using ECB makes it trivially easy to mix and match between pieces of separately encoded messages at block boundaries like above with DES. So, we can conclude that this is a property of ECB, not of AES or DES in particular.

Exercise_3_A

Let’s start with the factorization of N.Thus (module in RSA method) N is small the factorization is easy and by using just brute force algorithm we end up with 1st prime p=19 and second prime q=83.


Algorithms for factorization

[✓ Brute-force]

Brent

Pollard

Williams

Lenstra

Quadratic sieve

Input

Enter the number to be factorized: 1577

Factorization (stepwise)

Click "Continue" to factor the input number. If the result (shown below) can be factored further, click the button again to execute the factorization.

Factorization

The factorization is represented in the format <z1^a1 * z2^a2 *.... * zn^an>.
Composite numbers are highlighted in red.

Last factorization through: Brute Force Found 2 factors in 0.023 seconds.

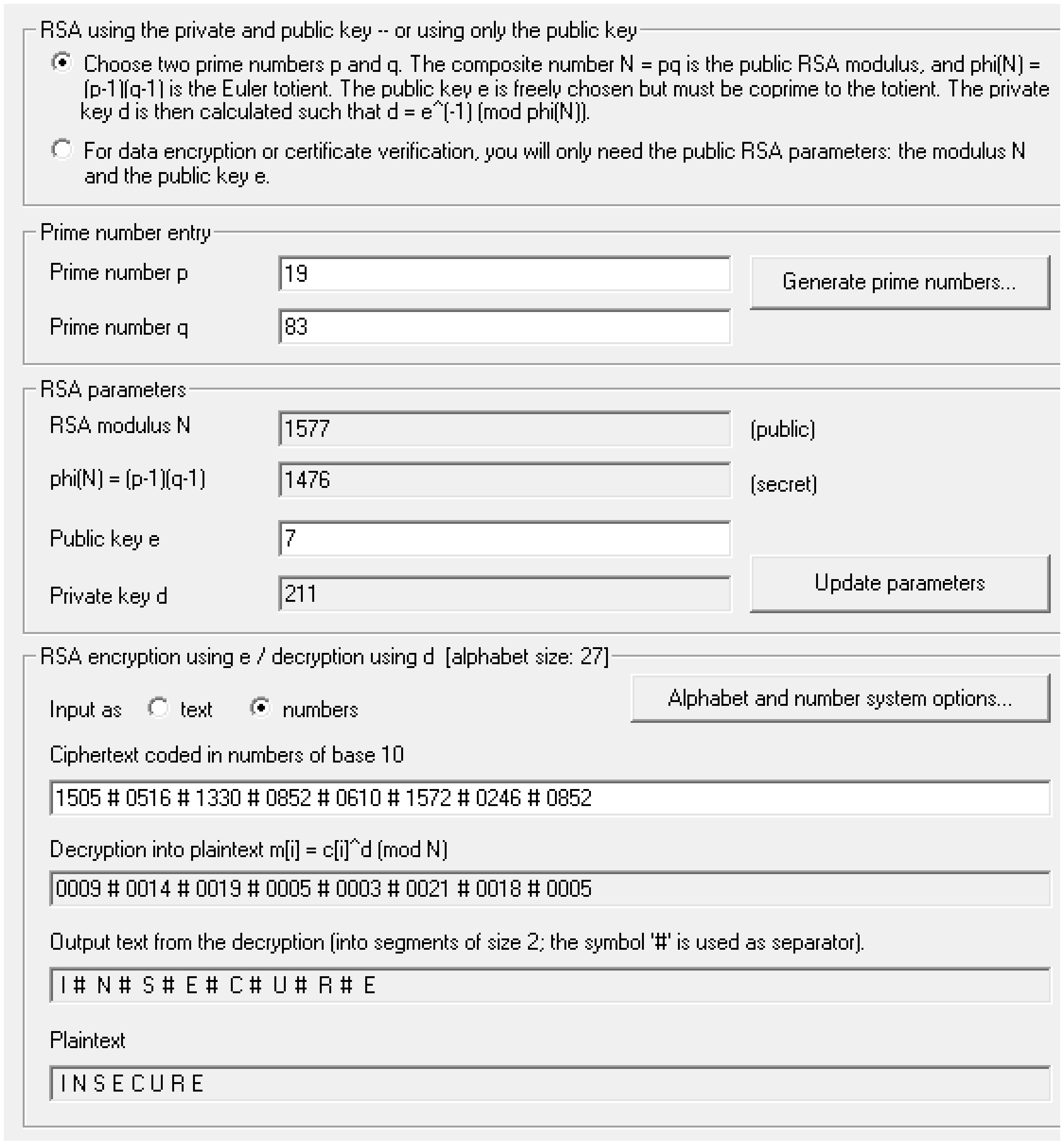
Factorization result: 19 * 83

We see that the two primes are different so we can continue(if the primes are equal it will not work).Then having the knowledge about p and q and because they are different we are able to calculate ϕ(n) = (p-1) x (q-1) known as Euler ϕ function.

$\phi(n) = (p - 1) \times (q - 1) \rightarrow 1476$ and by applying the above to the following formula $e \times d = 1 \pmod{\phi(n)}$ and Since by definition e and φ(N) are coprime then with extended euclidean algorithm you can find such d: $ed+k\varphi(N)=1$. For the chosen values of p, q, and e, we get d as:
d = 211

By having the private key d and by specifying the alphabet in the cryptool we are able to decrypt the message as per the image below.

RSA Demonstration



RSA using the private and public key -- or using only the public key

[✓] Choose two prime numbers p and q. The composite number N = pq is the public RSA modulus, and phi(N) = (p-1)(q-1) is the Euler totient. The public key e is freely chosen but must be coprime to the totient. The private key d is then calculated such that d = e^(-1) (mod phi(N)).

[ ] For data encryption or certificate verification, you will only need the public RSA parameters: the modulus N and the public key e.

Prime number entry

Prime number p: 19

Prime number q: 83

RSA parameters

RSA modulus N: 1577 (public)

phi(N) = (p-1)(q-1): 1476 (secret)

Public key e: 7

Private key d: 211

RSA encryption using e / decryption using d [alphabet size: 27]

Input as text [✓ numbers]

Ciphertext coded in numbers of base 10

```
1505 # 0516 # 1330 # 0852 # 0610 # 1572 # 0246 # 0852
```

Decryption into plaintext m[i] = c[i]^d (mod N)

```
0009 # 0014 # 0019 # 0005 # 0003 # 0021 # 0018 # 0005
```

Output text from the decryption (into segments of size 2; the symbol '#' is used as separator).

```
I # N # S # E # C # U # R # E
```

Plaintext

```
I N S E C U R E
```

Exercise_3_B

At first we have N = 1577 and e = 7 and the maximum number in the ciphertext representing the plaintext is between 0 and N-1 we can use Plain RSA and we can get the plaintext M from the ciphertext C through the following formula : C = M^e mod N and by solving with respect to M we get the plaintext for every encrypted number in the ciphertext as per the below links :

M[0] , M[1], M[2], M[3], M[4], M[5], M[6], M[7]

Exercise_4

Message Authentication Code (MAC) is cryptographic code, calculated by given key and given message:

auth_code = MAC(key, msg)

Typically, it behaves like a hash function: a minor change in the message or in the key results to totally different MAC value. It should be practically infeasible to change the key or the message and get the same MAC value. MAC codes, like hashes, are irreversible: it is impossible to recover the original message or the key from the MAC code. MAC algorithms are also known as "keyed hash functions", because they behave like a hash function with a key.

With the specific MAC algorithm if we were able to create a message with the same H(M) (To achieve sha-1 signatures to collide) it would be possible to extract the aes key and then via decryption, the mac key.In such scenario an attacker will have all the information in order to send a message that will be accepted in the destination.

However, the only concrete SHA1 collision to date was Google's.If cryptoanalysis advances, an attacker might be able to create inputs that deliberately collide. Currently, however, there is no known way to do this efficiently. For example Google needed 110 GPUs running for one year with an algorithm they implemented called “SHA-1 Shattered” (with brute force in order to achieve it in one year would need 12.000.000 CPUs).So in a feasible amount of time and expenses it is not possible neither to find the secret key nor to compute another valid pair.