**Kabeer Ahmed SE-19028**

# LAB 7

## Exercise:

### 1. What are ECB and CBC and their purpose? How do they differ?

ECB (Electronic Codebook) is essentially the first generation of the AES. It is the most basic form of block cipher encryption. CBC (Cipher Blocker Chaining) is an advanced form of block cipher encryption. With CBC mode encryption, each ciphertext block is dependent on all plaintext blocks processed up to that point.

ECB mode's issues arise from the fact that each block of the plaintext is encrypted completely independently. CBC mode eliminates this problem by carrying information from the encryption or decryption of one block to the next.

### 2. Why are the following keys considered to be weak keys of DES. Think about applying these keys to cryptool preferably trying to encrypt text with these keys twice.

**K1= 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1**

**K2= F E F E F E F E F E F E F E F E**

**K3= 1 F 1 F 1 F 1 F 0 E 0 E 0 E 0 E**

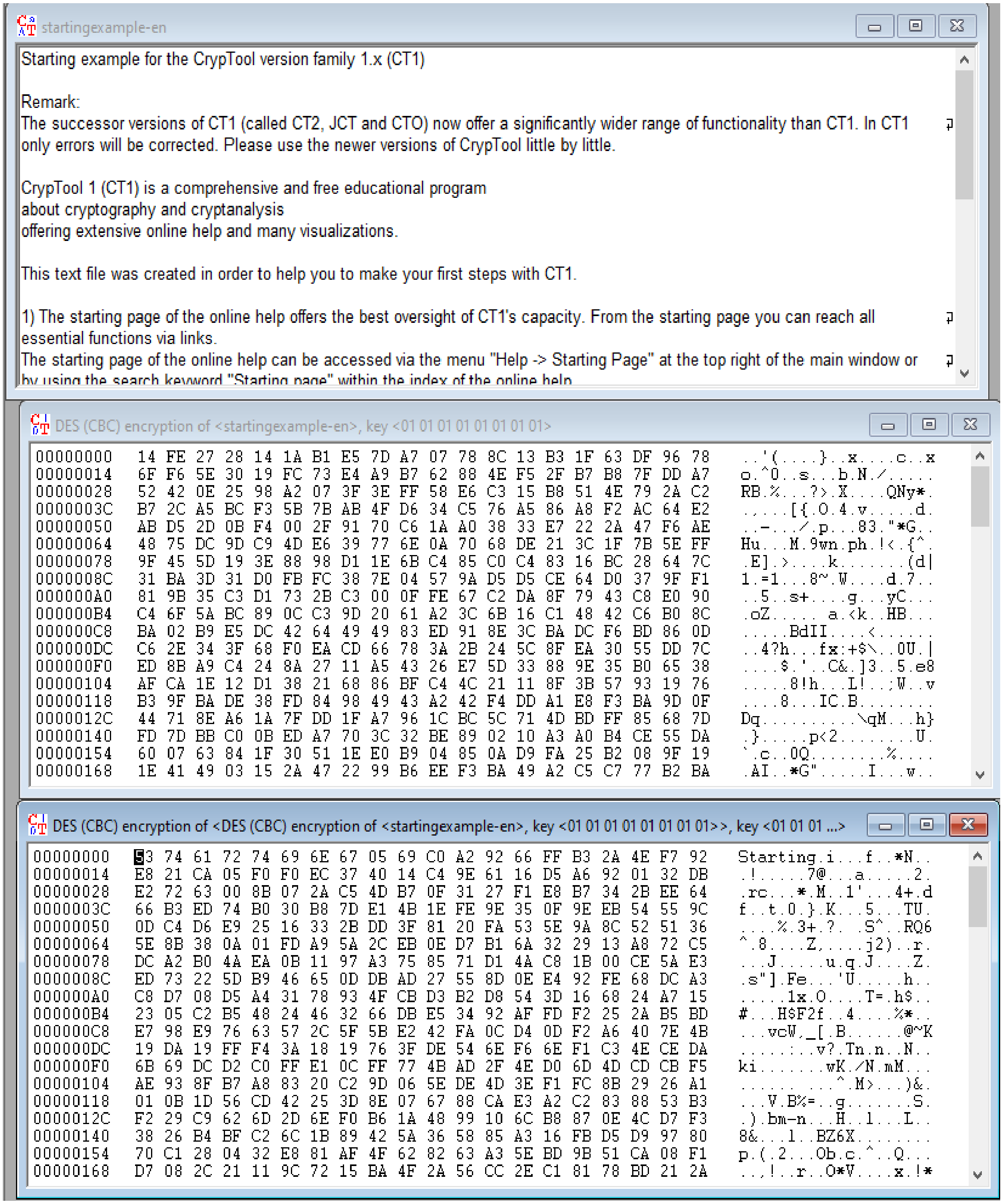
**K4= E 0 E 0 E 0 E 0 F 1 F 1 F 1 F 1**

This is weak keys because one reason is that after applying this twice we get some plaintext in the ciphertext and the other reason is that applying same key twice with DES gives the plaintext.

For

**Kabeer Ahmed SE-19028**

K1= 01 01 01 01 01 01 01 01



startingexample-en

Starting example for the CrypTool version family 1.x (CT1)

Remark:
The successor versions of CT1 (called CT2, JCT and CTO) now offer a significantly wider range of functionality than CT1. In CT1 only errors will be corrected. Please use the newer versions of CrypTool little by little.

CrypTool 1 (CT1) is a comprehensive and free educational program
about cryptography and cryptanalysis
offering extensive online help and many visualizations.

This text file was created in order to help you to make your first steps with CT1.

1) The starting page of the online help offers the best oversight of CT1's capacity. From the starting page you can reach all essential functions via links.
The starting page of the online help can be accessed via the menu "Help -> Starting Page" at the top right of the main window or by using the search keyword "Starting page" within the index of the online help.

DES (CBC) encryption of <startingexample-en>, key <01 01 01 01 01 01 01 01>

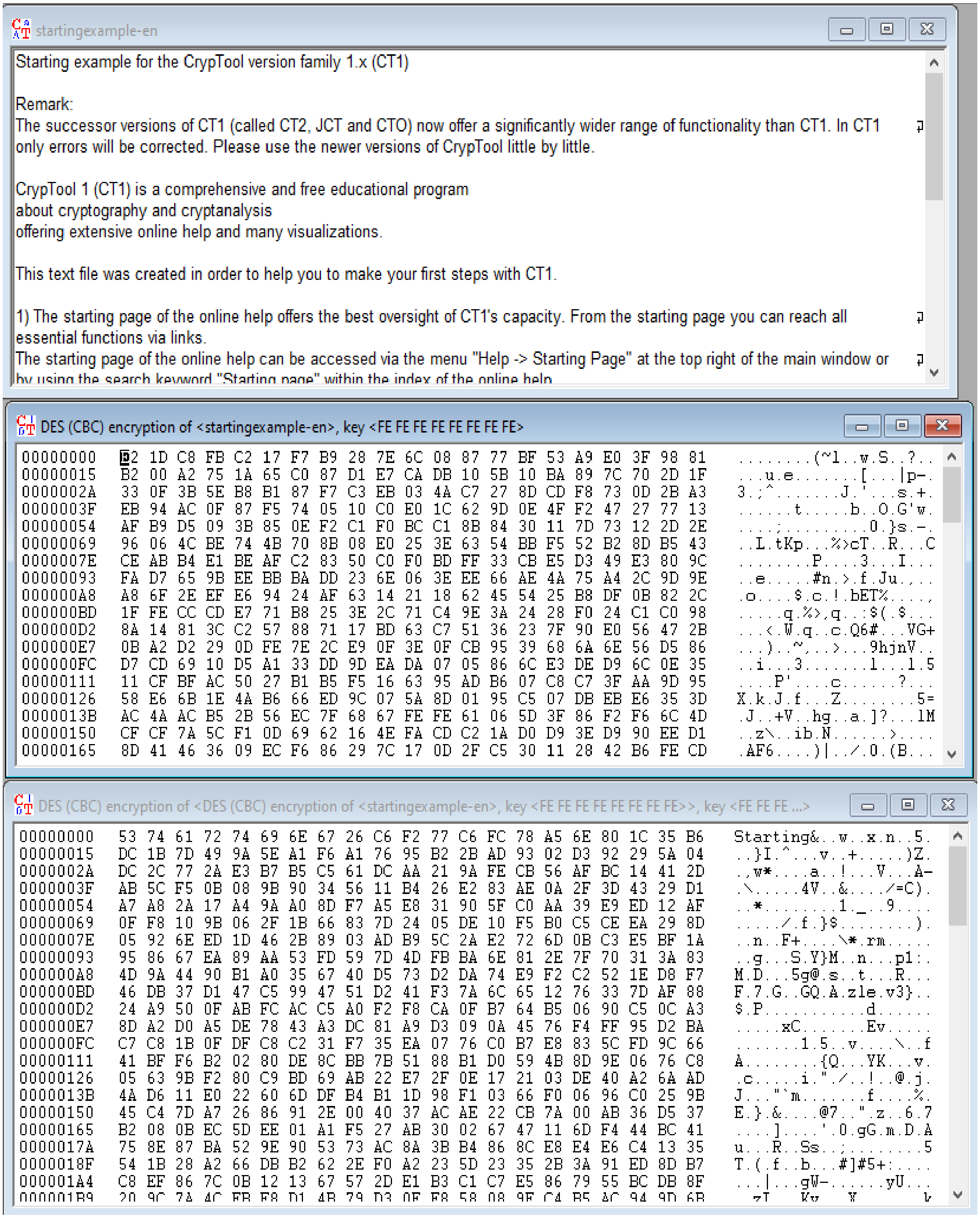
```
00000000   14 FE 27 28 14 1A B1 E5 7D A7 07 78 8C 13 B3 1F 63 DF 96 78   ..'(....}..x....c..x
00000014   6F F6 5E 30 19 FC 73 E4 A9 B7 62 88 4E F5 2F B7 B8 7F DD A7   o.^0..s...b.N./.....
00000028   52 42 0E 25 98 A2 07 3F 3E FF 58 E6 C3 15 B8 51 4E 79 2A C2   RB.%...?>.X....QNy*.
0000003C   B7 2C A5 BC F3 5B 7B AB 4F D6 34 C5 76 A5 86 A8 F2 AC 64 E2   .,...[{.O.4.v.....d.
00000050   AB D5 2D 0B F4 00 2F 91 70 C6 1A A0 38 33 E7 22 2A 47 F6 AE   ..-.../.p...83."*G..
00000064   48 75 DC 9D C9 4D E6 39 77 6E 0A 70 68 DE 21 3C 1F 7B 5E FF   Hu...M.9wn.ph.!<.{^.
00000078   9F 45 5D 19 3E 88 98 D1 1E 6B C4 85 C0 C4 83 16 BC 28 64 7C   .E].>....k.......(d|
0000008C   31 BA 3D 31 D0 FB FC 38 7E 04 57 9A D5 D5 CE 64 D0 37 9F F1   1.=1...8~.W....d.7..
000000A0   81 9B 35 C3 D1 73 2B C3 00 0F FE 67 C2 DA 8F 79 43 C8 E0 90   ..5..s+....g...yC...
000000B4   C4 6F 5A BC 89 0C C3 9D 20 61 A2 3C 6B 16 C1 48 42 C6 B0 8C   .oZ..... a.<k..HB...
000000C8   BA 02 B9 E5 DC 42 64 49 49 83 ED 91 8E 3C BA DC F6 BD 86 0D   .....BdII....<......
000000DC   C6 2E 34 3F 68 F0 EA CD 66 78 3A 2B 24 5C 8F EA 30 55 DD 7C   ..4?h...fx:+$\..0U.|
000000F0   ED 8B A9 C4 24 8A 27 11 A5 43 26 E7 5D 33 88 9E 35 B0 65 38   ....$.'..C&.]3..5.e8
00000104   AF CA 1E 12 D1 38 21 68 86 BF C4 4C 21 11 8F 3B 57 93 19 76   .....8!h...L!..;W..v
00000118   B3 9F BA DE 38 FD 84 98 49 43 A2 42 F4 DD A1 E8 F3 BA 9D 0F   ....8...IC.B........
0000012C   44 71 8E A6 1A 7F DD 1F A7 96 1C BC 5C 71 4D BD FF 85 68 7D   Dq..........\qM...h}
00000140   FD 7D BB C0 0B ED A7 70 3C 32 BE 89 02 10 A3 A0 B4 CE 55 DA   .}.....p<2........U.
00000154   60 07 63 84 1F 30 51 1E E0 B9 04 85 0A D9 FA 25 B2 08 9F 19   `.c..0Q........%....
00000168   1E 41 49 03 15 2A 47 22 99 B6 EE F3 BA 49 A2 C5 C7 77 B2 BA   .AI..*G".....I...w..
```

DES (CBC) encryption of <DES (CBC) encryption of <startingexample-en>, key <01 01 01 01 01 01 01 01>>, key <01 01 01 ...>

```
00000000   53 74 61 72 74 69 6E 67 05 69 C0 A2 92 66 FF B3 2A 4E F7 92   Starting.i...f..*N..
00000014   E8 21 CA 05 F0 F0 EC 37 40 14 C4 9E 61 16 D5 A6 92 01 32 DB   .!.....7@...a.....2.
00000028   E2 72 63 00 8B 07 2A C5 4D B7 0F 31 27 F1 E8 B7 34 2B EE 64   .rc...*.M..1'...4+.d
0000003C   66 B3 ED 74 B0 30 B8 7D E1 4B 1E FE 9E 35 0F 9E EB 54 55 9C   f..t.0.}.K...5...TU.
00000050   0D C4 D6 E9 25 16 33 2B DD 3F 81 20 FA 53 5E 9A 8C 52 51 36   ....%.3+.?. .S^..RQ6
00000064   5E 8B 38 0A 01 FD A9 5A 2C EB 0E D7 B1 6A 32 29 13 A8 72 C5   ^.8....Z,....j2)..r.
00000078   DC A2 B0 4A EA 0B 11 97 A3 75 85 71 D1 4A C8 1B 00 CE 5A E3   ...J.....u.q.J....Z.
0000008C   ED 73 22 5D B9 46 65 0D DB AD 27 55 8D 0E E4 92 FE 68 DC A3   .s"].Fe...'U.....h..
000000A0   C8 D7 08 D5 A4 31 78 93 4F CB D3 B2 D8 54 3D 16 68 24 A7 15   .....1x.O....T=.h$..
000000B4   23 05 C2 B5 48 24 46 32 66 DB E5 34 92 AF FD F2 25 2A B5 BD   #...H$F2f..4....%*..
000000C8   E7 98 E9 76 63 57 2C 5F 5B E2 42 FA 0C D4 0D F2 A6 40 7E 4B   ...vcW,_[.B......@~K
000000DC   19 DA 19 FF F4 3A 18 19 76 3F DE 54 6E F6 6E F1 C3 4E CE DA   .....:..v?.Tn.n..N..
000000F0   6B 69 DC D2 C0 FF E1 0C FF 77 4B AD 2F 4E D0 6D 4D CD CB F5   ki.......wK./N.mM...
00000104   AE 93 8F B7 A8 83 20 C2 9D 06 5E DE 4D 3E F1 FC 8B 29 26 A1   ...... ...^.M>...)&.
00000118   01 0B 1D 56 CD 42 25 3D 8E 07 67 88 CA E3 A2 C2 83 88 53 B3   ...V.B%=..g.......S.
0000012C   F2 29 C9 62 6D 2D 6E F0 B6 1A 48 99 10 6C B8 87 0E 4C D7 F3   .).bm-n...H..l...L..
00000140   38 26 B4 BF C2 6C 1B 89 42 5A 36 58 85 A3 16 FB D5 D9 97 80   8&...l..BZ6X........
00000154   70 C1 28 04 32 E8 81 AF 4F 62 82 63 A3 5E BD 9B 51 CA 08 F1   p.(.2...Ob.c.^..Q...
00000168   D7 08 2C 21 11 9C 72 15 BA 4F 2A 56 CC 2E C1 81 78 BD 21 2A   ..,!..r..O*V....x.!*
```

**Kabeer Ahmed  SE-19028**

K2 = FE FE FE FE FE FE FE FE



startingexample-en

Starting example for the CrypTool version family 1.x (CT1)

Remark:
The successor versions of CT1 (called CT2, JCT and CTO) now offer a significantly wider range of functionality than CT1. In CT1 only errors will be corrected. Please use the newer versions of CrypTool little by little.

CrypTool 1 (CT1) is a comprehensive and free educational program
about cryptography and cryptanalysis
offering extensive online help and many visualizations.

This text file was created in order to help you to make your first steps with CT1.

1) The starting page of the online help offers the best oversight of CT1's capacity. From the starting page you can reach all essential functions via links.
The starting page of the online help can be accessed via the menu "Help -> Starting Page" at the top right of the main window or by using the search keyword "Starting page" within the index of the online help

DES (CBC) encryption of <startingexample-en>, key <FE FE FE FE FE FE FE FE>

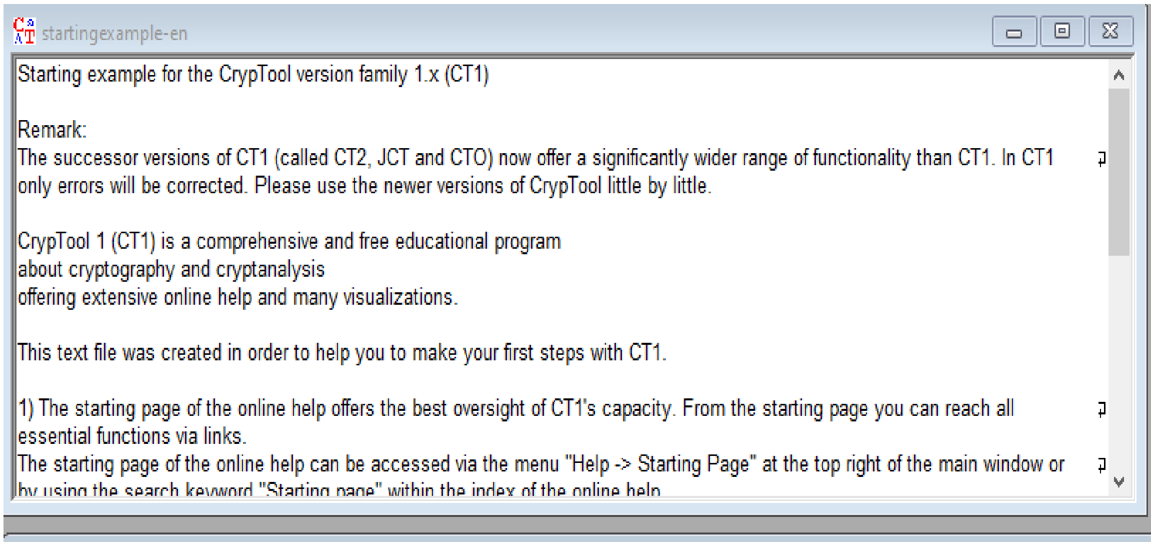
```
00000000   E2 1D C8 FB C2 17 F7 B9 28 7E 6C 08 87 77 BF 53 A9 E0 3F 98 81   ........(~l..w.S..?..
00000015   B2 00 A2 75 1A 65 C0 87 D1 E7 CA DB 10 5B 10 BA 89 7C 70 2D 1F   ...u.e.......[...|p-.
0000002A   33 0F 3B 5E B8 B1 87 F7 C3 EB 03 4A C7 27 8D CD F8 73 0D 2B A3   3.;^.......J.'...s.+.
0000003F   EB 94 AC 0F 87 F5 74 05 10 C0 E0 1C 62 9D 0E 4F F2 47 27 77 13   ......t.....b..O.G'w.
00000054   AF B9 D5 09 3B 85 0E F2 C1 F0 BC C1 8B 84 30 11 7D 73 12 2D 2E   ....;...........0.}s.-.
00000069   96 06 4C BE 74 4B 70 8B 08 E0 25 3E 63 54 BB F5 52 B2 8D B5 43   ..L.tKp...%>cT..R...C
0000007E   CE AB B4 E1 BE AF C2 83 50 C0 F0 BD FF 33 CB E5 D3 49 E3 80 9C   ........P....3...I...
00000093   FA D7 65 9B EE BB BA DD 23 6E 06 3E EE 66 AE 4A 75 A4 2C 9D 9E   ..e.....#n.>.f.Ju.,..
000000A8   A8 6F 2E EF E6 94 24 AF 63 14 21 18 62 45 54 25 B8 DF 0B 82 2C   .o....$.c.!.bET%....,
000000BD   1F FE CC CD E7 71 B8 25 3E 2C 71 C4 9E 3A 24 28 F0 24 C1 C0 98   .....q.%>,q..:$(.$...
000000D2   8A 14 81 3C C2 57 88 71 17 BD 63 C7 51 36 23 7F 90 E0 56 47 2B   ...<.W.q..c.Q6#...VG+
000000E7   0B A2 D2 29 0D FE 7E 2C E9 0F 3E 0F CB 95 39 68 6A 6E 56 D5 86   ...)..~,..>...9hjnV..
000000FC   D7 CD 69 10 D5 A1 33 DD 9D EA DA 07 05 86 6C E3 DE D9 6C 0E 35   ..i...3.......l...l.5
00000111   11 CF BF AC 50 27 B1 B5 F5 16 63 95 AD B6 07 C8 C7 3F AA 9D 95   ....P'....c......?...
00000126   58 E6 6B 1E 4A B6 66 ED 9C 07 5A 8D 01 95 C5 07 DB EB E6 35 3D   X.k.J.f...Z........5=
0000013B   AC 4A AC B5 2B 56 EC 7F 68 67 FE FE 61 06 5D 3F 86 F2 F6 6C 4D   .J..+V..hg..a.]?...lM
00000150   CF CF 7A 5C F1 0D 69 62 16 4E FA CD C2 1A D0 D9 3E D9 90 EE D1   ..z\..ib.N......>....
00000165   8D 41 46 36 09 EC F6 86 29 7C 17 0D 2F C5 30 11 28 42 B6 FE CD   .AF6....)|../.0.(B...
```

DES (CBC) encryption of <DES (CBC) encryption of <startingexample-en>, key <FE FE FE FE FE FE FE FE>>, key <FE FE FE ...>

```
00000000   53 74 61 72 74 69 6E 67 26 C6 F2 77 C6 FC 78 A5 6E 80 1C 35 B6   Starting&..w..x.n..5.
00000015   DC 1B 7D 49 9A 5E A1 F6 A1 76 95 B2 2B AD 93 02 D3 92 29 5A 04   ..}I.^...v..+.....)Z.
0000002A   DC 2C 77 2A E3 B7 B5 C5 61 DC AA 21 9A FE CB 56 AF BC 14 41 2D   .,w*....a..!...V...A-
0000003F   AB 5C F5 0B 08 9B 90 34 56 11 B4 26 E2 83 AE 0A 2F 3D 43 29 D1   .\.....4V..&..../=C).
00000054   A7 A8 2A 17 A4 9A A0 8D F7 A5 E8 31 90 5F C0 AA 39 E9 ED 12 AF   ..*........1._..9....
00000069   0F F8 10 9B 06 2F 1B 66 83 7D 24 05 DE 10 F5 B0 C5 CE EA 29 8D   ...../.f.}$........).
0000007E   05 92 6E ED 1D 46 2B 89 03 AD B9 5C 2A E2 72 6D 0B C3 E5 BF 1A   ..n..F+....\*.rm.....
00000093   95 86 67 EA 89 AA 53 FD 59 7D 4D FB BA 6E 81 2E 7F 70 31 3A 83   ..g...S.Y}M..n...p1:.
000000A8   4D 9A 44 90 B1 A0 35 67 40 D5 73 D2 DA 74 E9 F2 C2 52 1E D8 F7   M.D...5g@.s..t...R...
000000BD   46 DB 37 D1 47 C5 99 47 51 D2 41 F3 7A 6C 65 12 76 33 7D AF 88   F.7.G..GQ.A.zle.v3}..
000000D2   24 A9 50 0F AB FC AC C5 A0 F2 F8 CA 0F B7 64 B5 06 90 C5 0C A3   $.P...........d......
000000E7   8D A2 D0 A5 DE 78 43 A3 DC 81 A9 D3 09 0A 45 76 F4 FF 95 D2 BA   .....xC.......Ev.....
000000FC   C7 C8 1B 0F DF C8 C2 31 F7 35 EA 07 76 C0 B7 E8 83 5C FD 9C 66   .......1.5..v....\..f
00000111   41 BF F6 B2 02 80 DE 8C BB 7B 51 88 B1 D0 59 4B 8D 9E 06 76 C8   A.........{Q...YK...v.
00000126   05 63 9B F2 80 C9 BD 69 AB 22 E7 2F 0E 17 21 03 DE 40 A2 6A AD   .c.....i."./..!..@.j.
0000013B   4A D6 11 E0 22 60 6D DF B4 B1 1D 98 F1 03 66 F0 06 96 C0 25 9B   J..."`m......f....%.
00000150   45 C4 7D A7 26 86 91 2E 00 40 37 AC AE 22 CB 7A 00 AB 36 D5 37   E.}.&....@7..".z..6.7
00000165   B2 08 0B EC 5D EE 01 A1 F5 27 AB 30 02 67 47 11 6D F4 44 BC 41   ....]....'.0.gG.m.D.A
0000017A   75 8E 87 BA 52 9E 90 53 73 AC 8A 3B B4 86 8C E8 E4 E6 C4 13 35   u...R..Ss..;........5
0000018F   54 1B 28 A2 66 DB B2 62 2E F0 A2 23 5D 23 35 2B 3A 91 ED 8D B7   T.(.f..b...#]#5+:....
000001A4   C8 EF 86 7C 0B 12 13 67 57 2D E1 B3 C1 C7 E5 86 79 55 BC DB 8F   ...|...gW-......yU...
000001B9   20 9C 7A 4C FB F8 D1 4B 79 D3 0F F8 58 08 9F C4 B5 AC 94 9D 6B    .zL....Ky...X.......k
```

**Kabeer Ahmed  SE-19028**

K3 = 1F 1F 1F 1F 0E 0E 0E 0E



startingexample-en

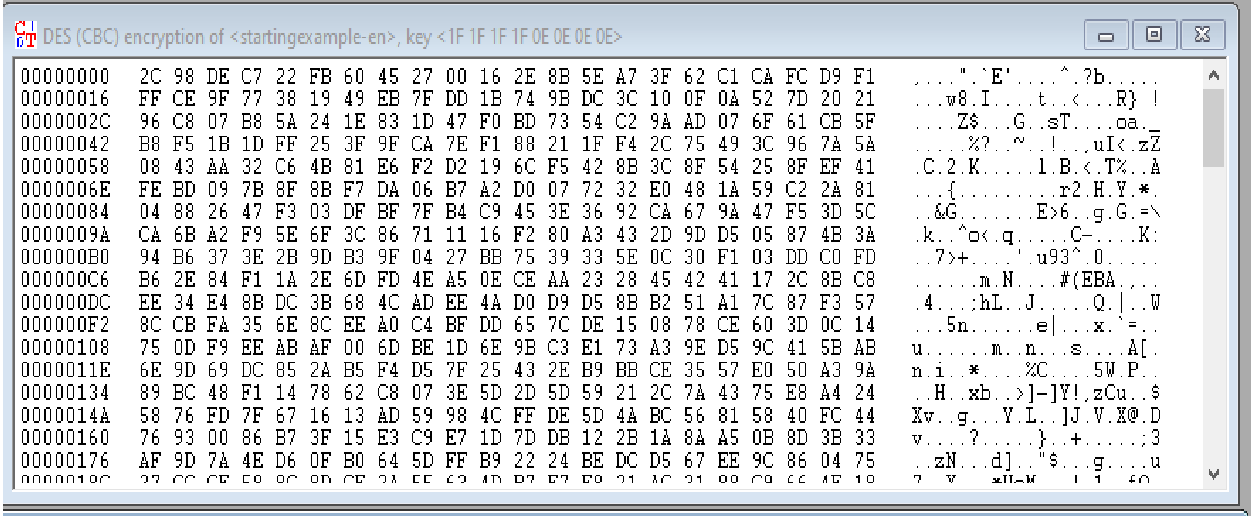
Starting example for the CrypTool version family 1.x (CT1)

Remark:
The successor versions of CT1 (called CT2, JCT and CTO) now offer a significantly wider range of functionality than CT1. In CT1 only errors will be corrected. Please use the newer versions of CrypTool little by little.

CrypTool 1 (CT1) is a comprehensive and free educational program
about cryptography and cryptanalysis
offering extensive online help and many visualizations.

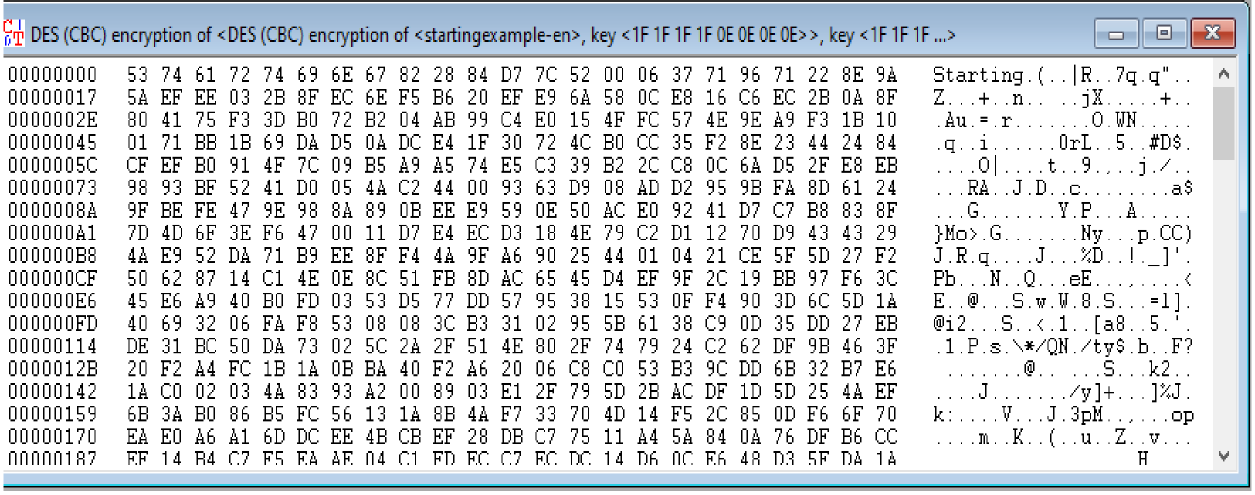
This text file was created in order to help you to make your first steps with CT1.

1) The starting page of the online help offers the best oversight of CT1's capacity. From the starting page you can reach all essential functions via links.
The starting page of the online help can be accessed via the menu "Help -> Starting Page" at the top right of the main window or by using the search keyword "Starting page" within the index of the online help



DES (CBC) encryption of <startingexample-en>, key <1F 1F 1F 1F 0E 0E 0E 0E>

```
00000000  2C 98 DE C7 22 FB 60 45 27 00 16 2E 8B 5E A7 3F 62 C1 CA FC D9 F1   ,...".`E'....^.?b.....
00000016  FF CE 9F 77 38 19 49 EB 7F DD 1B 74 9B DC 3C 10 0F 0A 52 7D 20 21   ...w8.I....t..<...R} !
0000002C  96 C8 07 B8 5A 24 1E 83 1D 47 F0 BD 73 54 C2 9A AD 07 6F 61 CB 5F   ....Z$...G..sT....oa._
00000042  B8 F5 1B 1D FF 25 3F 9F CA 7E F1 88 21 1F F4 2C 75 49 3C 96 7A 5A   .....%?..~..!..,uI<.zZ
00000058  08 43 AA 32 C6 4B 81 E6 F2 D2 19 6C F5 42 8B 3C 8F 54 25 8F EF 41   .C.2.K.....l.B.<.T%..A
0000006E  FE BD 09 7B 8F 8B F7 DA 06 B7 A2 D0 07 72 32 E0 48 1A 59 C2 2A 81   ...{.........r2.H.Y.*.
00000084  04 88 26 47 F3 03 DF BF 7F B4 C9 45 3E 36 92 CA 67 9A 47 F5 3D 5C   ..&G.......E>6..g.G.=\
0000009A  CA 6B A2 F9 5E 6F 3C 86 71 11 16 F2 80 A3 43 2D 9D D5 05 87 4B 3A   .k..^o<.q.....C-....K:
000000B0  94 B6 37 3E 2B 9D B3 9F 04 27 BB 75 39 33 5E 0C 30 F1 03 DD C0 FD   ..7>+....'.u93^.0.....
000000C6  B6 2E 84 F1 1A 2E 6D FD 4E A5 0E CE AA 23 28 45 42 41 17 2C 8B C8   ......m.N....#(EBA.,..
000000DC  EE 34 E4 8B DC 3B 68 4C AD EE 4A D0 D9 D5 8B B2 51 A1 7C 87 F3 57   .4...;hL..J.....Q.|..W
000000F2  8C CB FA 35 6E 8C EE A0 C4 BF DD 65 7C DE 15 08 78 CE 60 3D 0C 14   ...5n......e|...x.`=..
00000108  75 0D F9 EE AB AF 00 6D BE 1D 6E 9B C3 E1 73 A3 9E D5 9C 41 5B AB   u......m..n...s....A[.
0000011E  6E 9D 69 DC 85 2A B5 F4 D5 7F 25 43 2E B9 BB CE 35 57 E0 50 A3 9A   n.i..*....%C....5W.P..
00000134  89 BC 48 F1 14 78 62 C8 07 3E 5D 2D 5D 59 21 2C 7A 43 75 E8 A4 24   ..H..xb..>]-]Y!,zCu..$
0000014A  58 76 FD 7F 67 16 13 AD 59 98 4C FF DE 5D 4A BC 56 81 58 40 FC 44   Xv..g...Y.L..]J.V.X@.D
00000160  76 93 00 86 B7 3F 15 E3 C9 E7 1D 7D DB 12 2B 1A 8A A5 0B 8D 3B 33   v....?.....}..+.....;3
00000176  AF 9D 7A 4E D6 0F B0 64 5D FF B9 22 24 BE DC D5 67 EE 9C 86 04 75   ..zN...d].."$...g....u
```

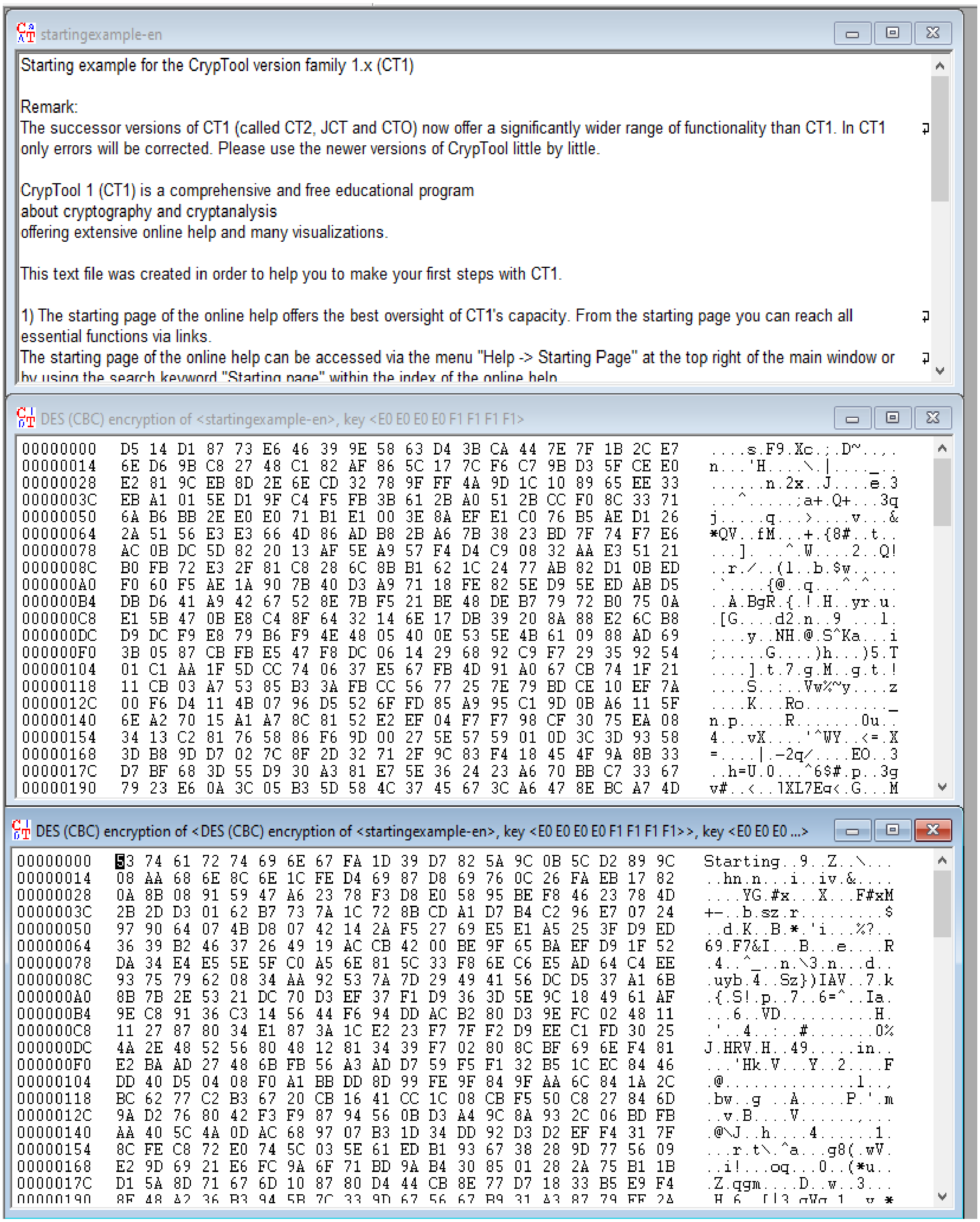


DES (CBC) encryption of <DES (CBC) encryption of <startingexample-en>, key <1F 1F 1F 1F 0E 0E 0E 0E>>, key <1F 1F 1F ...>

```
00000000  53 74 61 72 74 69 6E 67 82 28 84 D7 7C 52 00 06 37 71 96 71 22 8E 9A   Starting.(..|R..7q.q"..
00000017  5A EF EE 03 2B 8F EC 6E F5 B6 20 EF E9 6A 58 0C E8 16 C6 EC 2B 0A 8F   Z...+..n.. ..jX.....+..
0000002E  80 41 75 F3 3D B0 72 B2 04 AB 99 C4 E0 15 4F FC 57 4E 9E A9 F3 1B 10   .Au.=.r.......O.WN.....
00000045  01 71 BB 1B 69 DA D5 0A DC E4 1F 30 72 4C B0 CC 35 F2 8E 23 44 24 84   .q..i......0rL..5..#D$.
0000005C  CF EF B0 91 4F 7C 09 B5 A9 A5 74 E5 C3 39 B2 2C C8 0C 6A D5 2F E8 EB   ....O|....t..9.,..j./..
00000073  98 93 BF 52 41 D0 05 4A C2 44 00 93 63 D9 08 AD D2 95 9B FA 8D 61 24   ...RA..J.D..c........a$
0000008A  9F BE FE 47 9E 98 8A 89 0B EE E9 59 0E 50 AC E0 92 41 D7 C7 B8 83 8F   ...G.......Y.P...A.....
000000A1  7D 4D 6F 3E F6 47 00 11 D7 E4 EC D3 18 4E 79 C2 D1 12 70 D9 43 43 29   }Mo>.G.......Ny...p.CC)
000000B8  4A E9 52 DA 71 B9 EE 8F F4 4A 9F A6 90 25 44 01 04 21 CE 5F 5D 27 F2   J.R.q....J...%D..!._]'.
000000CF  50 62 87 14 C1 4E 0E 8C 51 FB 8D AC 65 45 D4 EF 9F 2C 19 BB 97 F6 3C   Pb...N..Q...eE...,....<
000000E6  45 E6 A9 40 B0 FD 03 53 D5 77 DD 57 95 38 15 53 0F F4 90 3D 6C 5D 1A   E..@...S.w.W.8.S...=l].
000000FD  40 69 32 06 FA F8 53 08 08 3C B3 31 02 95 5B 61 38 C9 0D 35 DD 27 EB   @i2...S..<.1..[a8..5.'.
00000114  DE 31 BC 50 DA 73 02 5C 2A 2F 51 4E 80 2F 74 79 24 C2 62 DF 9B 46 3F   .1.P.s.\*/QN./ty$.b..F?
0000012B  20 F2 A4 FC 1B 1A 0B BA 40 F2 A6 20 06 C8 C0 53 B3 9C DD 6B 32 B7 E6    .......@.. ...S...k2..
00000142  1A C0 02 03 4A 83 93 A2 00 89 03 E1 2F 79 5D 2B AC DF 1D 5D 25 4A EF   ....J......./y]+...]%J.
00000159  6B 3A B0 86 B5 FC 56 13 1A 8B 4A F7 33 70 4D 14 F5 2C 85 0D F6 6F 70   k:....V...J.3pM..,...op
00000170  EA E0 A6 A1 6D DC EE 4B CB EF 28 DB C7 75 11 A4 5A 84 0A 76 DF B6 CC   ....m..K..(..u..Z..v...
00000187  EF 14 B4 C7 F5 EA AE 04 C1 FD EC C7 EC DC 14 D6 0C E6 48 D3 5F DA 1A                     H
```

**Kabeer Ahmed  SE-19028**

K4 = E0 E0 E0 E0 F1 F1 F1 F1



Starting example for the CrypTool version family 1.x (CT1)

Remark:
The successor versions of CT1 (called CT2, JCT and CTO) now offer a significantly wider range of functionality than CT1. In CT1 only errors will be corrected. Please use the newer versions of CrypTool little by little.

CrypTool 1 (CT1) is a comprehensive and free educational program
about cryptography and cryptanalysis
offering extensive online help and many visualizations.

This text file was created in order to help you to make your first steps with CT1.

1) The starting page of the online help offers the best oversight of CT1's capacity. From the starting page you can reach all essential functions via links.
The starting page of the online help can be accessed via the menu "Help -> Starting Page" at the top right of the main window or by using the search keyword "Starting page" within the index of the online help

DES (CBC) encryption of <startingexample-en>, key <E0 E0 E0 E0 F1 F1 F1 F1>

```
00000000  D5 14 D1 87 73 E6 46 39 9E 58 63 D4 3B CA 44 7E 7F 1B 2C E7   ....s.F9.Xc.;.D~..,.
00000014  6E D6 9B C8 27 48 C1 82 AF 86 5C 17 7C F6 C7 9B D3 5F CE E0   n...'H....\.|...._..
00000028  E2 81 9C EB 8D 2E 6E CD 32 78 9F FF 4A 9D 1C 10 89 65 EE 33   ......n.2x..J....e.3
0000003C  EB A1 01 5E D1 9F C4 F5 FB 3B 61 2B A0 51 2B CC F0 8C 33 71   ...^.....;a+.Q+...3q
00000050  6A B6 BB 2E E0 E0 71 B1 E1 00 3E 8A EF E1 C0 76 B5 AE D1 26   j.....q...>....v...&
00000064  2A 51 56 E3 E3 66 4D 86 AD B8 2B A6 7B 38 23 BD 7F 74 F7 E6   *QV..fM...+.{8#..t..
00000078  AC 0B DC 5D 82 20 13 AF 5E A9 57 F4 D4 C9 08 32 AA E3 51 21   ...]. ..^.W....2..Q!
0000008C  B0 FB 72 E3 2F 81 C8 28 6C 8B B1 62 1C 24 77 AB 82 D1 0B ED   ..r./..(l..b.$w.....
000000A0  F0 60 F5 AE 1A 90 7B 40 D3 A9 71 18 FE 82 5E D9 5E ED AB D5   .`....{@..q...^.^...
000000B4  DB D6 41 A9 42 67 52 8E 7B F5 21 BE 48 DE B7 79 72 B0 75 0A   ..A.BgR.{.!.H..yr.u.
000000C8  E1 5B 47 0B E8 C4 8F 64 32 14 6E 17 DB 39 20 8A 88 E2 6C B8   .[G....d2.n..9 ...l.
000000DC  D9 DC F9 E8 79 B6 F9 4E 48 05 40 0E 53 5E 4B 61 09 88 AD 69   ....y..NH.@.S^Ka...i
000000F0  3B 05 87 CB FB E5 47 F8 DC 06 14 29 68 92 C9 F7 29 35 92 54   ;.....G....)h...)5.T
00000104  01 C1 AA 1F 5D CC 74 06 37 E5 67 FB 4D 91 A0 67 CB 74 1F 21   ....].t.7.g.M..g.t.!
00000118  11 CB 03 A7 53 85 B3 3A FB CC 56 77 25 7E 79 BD CE 10 EF 7A   ....S..:..Vw%~y....z
0000012C  00 F6 D4 11 4B 07 96 D5 52 6F FD 85 A9 95 C1 9D 0B A6 11 5F   ....K...Ro..........
00000140  6E A2 70 15 A1 A7 8C 81 52 E2 EF 04 F7 F7 98 CF 30 75 EA 08   n.p.....R.......0u..
00000154  34 13 C2 81 76 58 86 F6 9D 00 27 5E 57 59 01 0D 3C 3D 93 58   4...vX....'^WY..<=.X
00000168  3D B8 9D D7 02 7C 8F 2D 32 71 2F 9C 83 F4 18 45 4F 9A 8B 33   =....|.-2q/....EO..3
0000017C  D7 BF 68 3D 55 D9 30 A3 81 E7 5E 36 24 23 A6 70 BB C7 33 67   ..h=U.0....^6$#.p..3g
00000190  79 23 E6 0A 3C 05 B3 5D 58 4C 37 45 67 3C A6 47 8E BC A7 4D   y#..<..]XL7Eg<.G...M
```

DES (CBC) encryption of <DES (CBC) encryption of <startingexample-en>, key <E0 E0 E0 E0 F1 F1 F1 F1>>, key <E0 E0 E0 ...>

```
00000000  53 74 61 72 74 69 6E 67 FA 1D 39 D7 82 5A 9C 0B 5C D2 89 9C   Starting..9..Z..\...
00000014  08 AA 68 6E 8C 6E 1C FE D4 69 87 D8 69 76 0C 26 FA EB 17 82   ..hn.n...i..iv.&....
00000028  0A 8B 08 91 59 47 A6 23 78 F3 D8 E0 58 95 BE F8 46 23 78 4D   ....YG.#x...X...F#xM
0000003C  2B 2D D3 01 62 B7 73 7A 1C 72 8B CD A1 D7 B4 C2 96 E7 07 24   +-..b.sz.r.........$
00000050  97 90 64 07 4B D8 07 42 14 2A F5 27 69 E5 E1 A5 25 3F D9 ED   ..d.K..B.*.'i...%?..
00000064  36 39 B2 46 37 26 49 19 AC CB 42 00 BE 9F 65 BA EF D9 1F 52   69.F7&I...B...e....R
00000078  DA 34 E4 E5 5E 5F C0 A5 6E 81 5C 33 F8 6E C6 E5 AD 64 C4 EE   .4..^_..n.\3.n...d..
0000008C  93 75 79 62 08 34 AA 92 53 7A 7D 29 49 41 56 DC D5 37 A1 6B   .uyb.4..Sz})IAV..7.k
000000A0  8B 7B 2E 53 21 DC 70 D3 EF 37 F1 D9 36 3D 5E 9C 18 49 61 AF   .{.S!.p..7..6=^..Ia.
000000B4  9E C8 91 36 C3 14 56 44 F6 94 DD AC B2 80 D3 9E FC 02 48 11   ...6..VD..........H.
000000C8  11 27 87 80 34 E1 87 3A 1C E2 23 F7 7F F2 D9 EE C1 FD 30 25   .'..4..:..#.......0%
000000DC  4A 2E 48 52 56 80 48 12 81 34 39 F7 02 80 8C BF 69 6E F4 81   J.HRV.H..49.....in..
000000F0  E2 BA AD 27 48 6B FB 56 A3 AD D7 59 F5 F1 32 B5 1C EC 84 46   ...'Hk.V...Y..2....F
00000104  DD 40 D5 04 08 F0 A1 BB DD 8D 99 FE 9F 84 9F AA 6C 84 1A 2C   .@..............l..,
00000118  BC 62 77 C2 B3 67 20 CB 16 41 CC 1C 08 CB F5 50 C8 27 84 6D   .bw..g ..A.....P.'.m
0000012C  9A D2 76 80 42 F3 F9 87 94 56 0B D3 A4 9C 8A 93 2C 06 BD FB   ..v.B....V......,...
00000140  AA 40 5C 4A 0D AC 68 97 07 B3 1D 34 DD 92 D3 D2 EF F4 31 7F   .@\J..h....4......1.
00000154  8C FE C8 72 E0 74 5C 03 5E 61 ED B1 93 67 38 28 9D 77 56 09   ...r.t\.^a...g8(.wV.
00000168  E2 9D 69 21 E6 FC 9A 6F 71 BD 9A B4 30 85 01 28 2A 75 B1 1B   ..i!...oq...0..(*u..
0000017C  D1 5A 8D 71 67 6D 10 87 80 D4 44 CB 8E 77 D7 18 33 B5 E9 F4   .Z.qgm....D..w..3...
00000190  8F 48 A2 36 B3 94 5B 7C 33 9D 67 56 67 B9 31 A3 87 79 FF 2A   .H.6..[|3.gVg.1..y.*
```