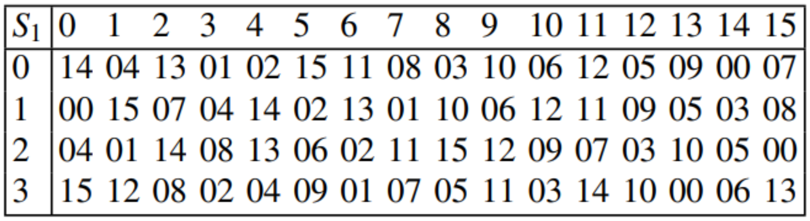
**Aria Javani**

**9725303**

## 1.3.1 :

**Table 3.4** S-box $S_1$



| $S_1$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 14 | 04 | 13 | 01 | 02 | 15 | 11 | 08 | 03 | 10 | 06 | 12 | 05 | 09 | 00 | 07 |
| 1 | 00 | 15 | 07 | 04 | 14 | 02 | 13 | 01 | 10 | 06 | 12 | 11 | 09 | 05 | 03 | 08 |
| 2 | 04 | 01 | 14 | 08 | 13 | 06 | 02 | 11 | 15 | 12 | 09 | 07 | 03 | 10 | 05 | 00 |
| 3 | 15 | 12 | 08 | 02 | 04 | 09 | 01 | 07 | 05 | 11 | 03 | 14 | 10 | 00 | 06 | 13 |

Calculating the $S_1$ for numbers using the above table

1.

$$S_1(000000) \oplus S_1(000001) = 14 \oplus 0 = 14$$

$$S_1(000000 \oplus 000001) = 0$$

2.

$$S_1(111111) \oplus S_1(100000) = 13 \oplus 4 = 1$$

$$S_1(111111 \oplus 100000) = 8$$

3.

$$S_1(101010) \oplus S_1(010101) = 6 \oplus 9 = 15$$

$$S_1(101010 \oplus 010101) = 13$$

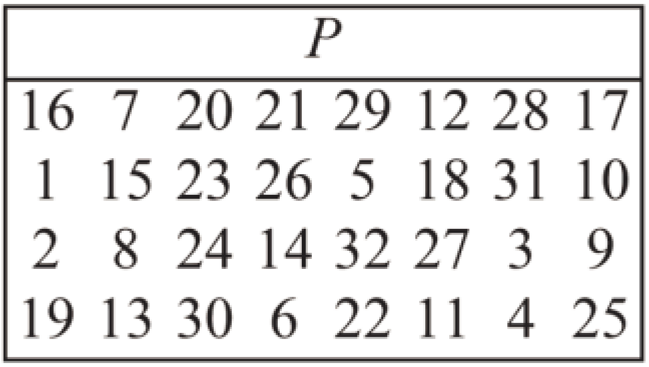
## 1.3.3 :

we procced step by step :

initial permutation : after this part text is still all zero

splitting into two parts : first 32 bits bits remain untouched and rest of the bits enter next phase.

calculating f function : first we have to expand our 32 bit input into 48 after this operation we have 48 bits of zeros. after that we do the binary summation on this generated bits and deprived key which leaves us with 48 bits zeros again. in the next step we have to devide these 48 bits by 8 and send each group to one of the S boxes then combine the outputs. output after this part will be 1110,1111,1010,0111,0010,1100,0100,1101 then we have to permute this output using the below table



| *P* | | | | | | | |
|---|---|---|---|---|---|---|---|
| 16 | 7 | 20 | 21 | 29 | 12 | 28 | 17 |
| 1 | 15 | 23 | 26 | 5 | 18 | 31 | 10 |
| 2 | 8 | 24 | 14 | 32 | 27 | 3 | 9 |
| 19 | 13 | 30 | 6 | 22 | 11 | 4 | 25 |

result : 1111,0101,0111,1100,0110,1001,1110,0010

final operation :

in this part first we xor the ouput of f with left part of the input then swap two separated parts. the output will be

0000,0000,0000,0000,0000,0000,0000,0000,
1111,0101,0111,1100,0110,1001,1110,0010

**1.3.5 :**

after initial permutation the new position of our 1 bit will be 33th bit so it takes place in the second half of the whole text. in the next step the text will be expanded which causes us to have 1 on the second and 48th bits so

1. two S boxes(1 and 8) will get different inputs
2. 3 for the first 6 bits and 2 for the last 6 bits → 5bits total
3. 0011,1111,1010,0111,0010,1100,0100,0001 after s boxes → 1011,0101,0010,1100,0010,1001,1111,0010 after permutation
4. due to the previous question 5bits

**1.3.7 :**

1. all subkeys are identical when the key is weak.

2.

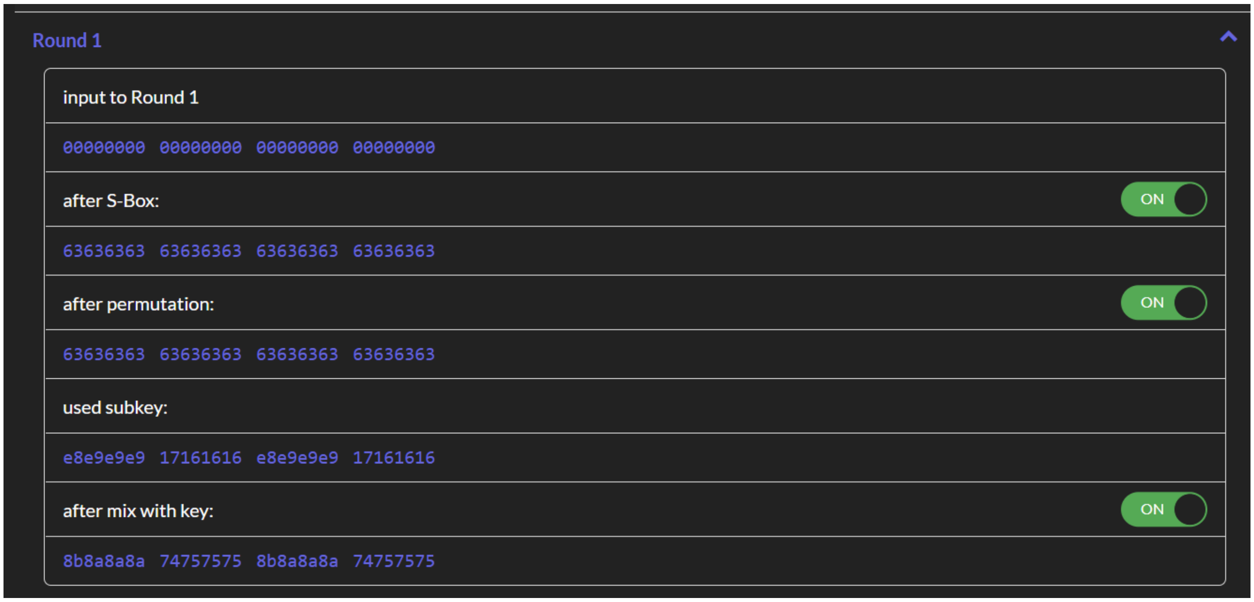
$$k_{i+1} = k_{16-i}$$

- alternating ones+zeros(exp: 0x0101010101010101)
- alternating F+E(exp: 0xFEFEFEFEFEFEFEFE)
- 0x(E0E0E0E0F1F1F1 F1)
- 0x(1F1F1F1F0E0E0E0E)

3. $\frac{4}{2^{56}}$=$\frac{1}{2^{54}}$

**1.4.9 :**

8b8a8a8a747575758b8a8a8a74757575



Round 1

input to Round 1

```
00000000 00000000 00000000 00000000
```

after S-Box: ON

```
63636363 63636363 63636363 63636363
```

after permutation: ON

```
63636363 63636363 63636363 63636363
```

used subkey:

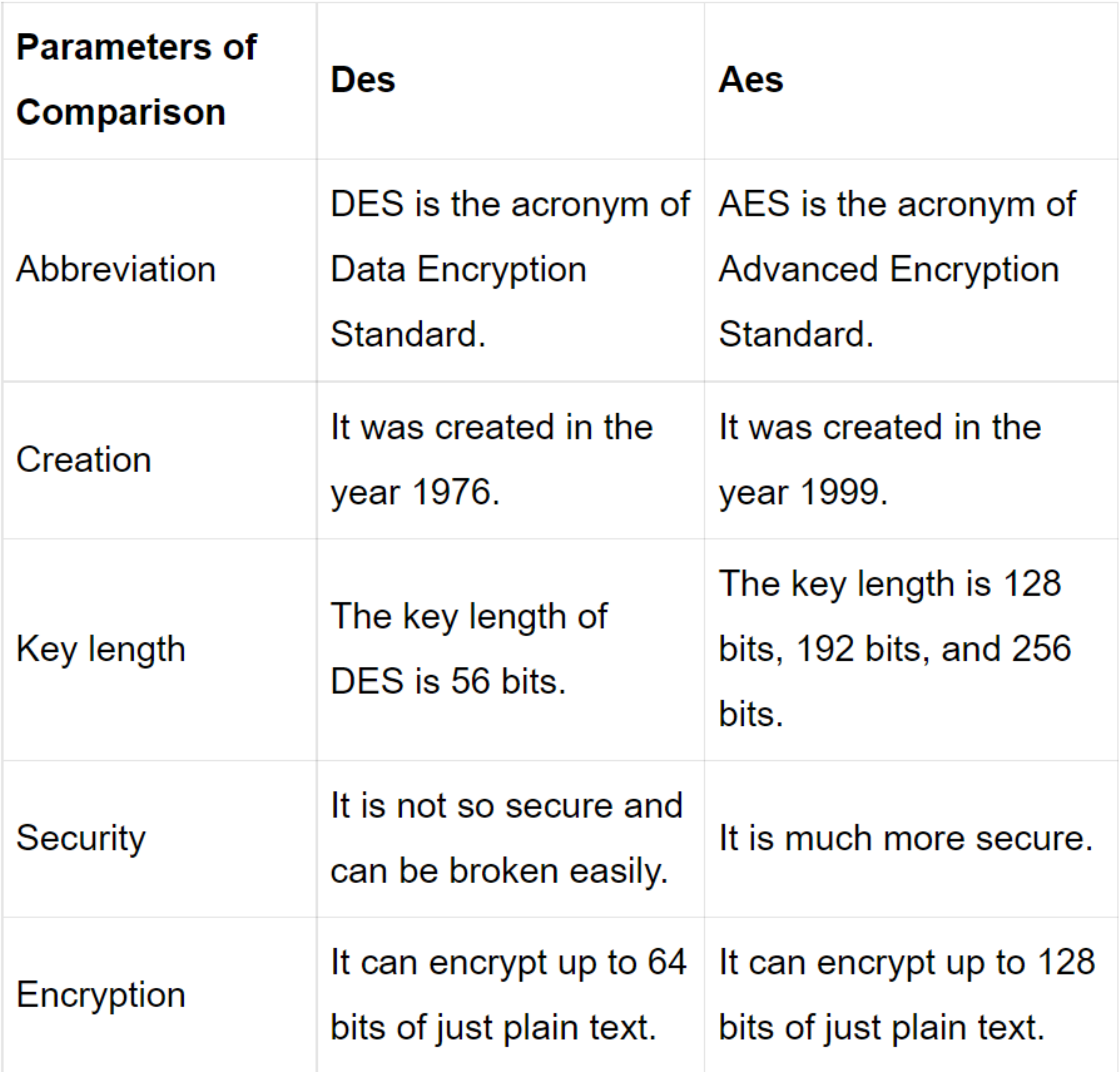
```
e8e9e9e9 17161616 e8e9e9e9 17161616
```

after mix with key: ON

```
8b8a8a8a 74757575 8b8a8a8a 74757575
```

**2:**

a. block ciphers break down the plain text into individual blocks then cipher those blocks bit by bit but stream ciphers cipher the whole plain text bit by bit.
b. to add the confusion feature.
c. since all the process is consist of either permutation which is reversible and xor which we have the $a \oplus b = c \rightarrow a = b \oplus c$ then des decryption is indeed reverse of des encryption.
d. AES is stronger against all kind of attacks since has both longer key and more complicated operations.



| Parameters of Comparison | Des | Aes |
|---|---|---|
| Abbreviation | DES is the acronym of Data Encryption Standard. | AES is the acronym of Advanced Encryption Standard. |
| Creation | It was created in the year 1976. | It was created in the year 1999. |
| Key length | The key length of DES is 56 bits. | The key length is 128 bits, 192 bits, and 256 bits. |
| Security | It is not so secure and can be broken easily. | It is much more secure. |
| Encryption | It can encrypt up to 64 bits of just plain text. | It can encrypt up to 128 bits of just plain text. |

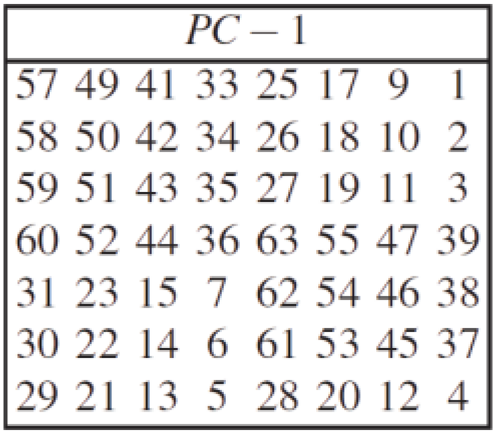
e.

i) Add RoundKey
ii) Add RoundKey
iii) SubBytes
iv) MixColumns
v) ShiftRows

**3.1 :** key and text : 0000 0001 0010 0011 0100 0101 0110 0111 1000 1001 1010 1011 1100 1101 1110 1111

**attention : we didn’t use initial and final permutations since question hasn’t mentioned it.

a.

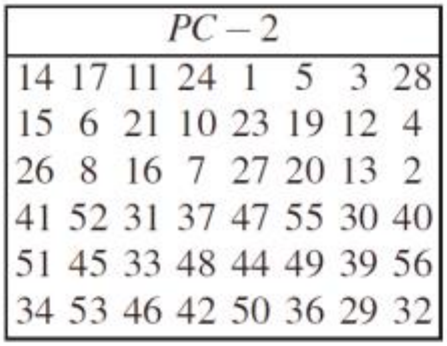


| PC − 1 | | | | | | | |
|---|---|---|---|---|---|---|---|
| 57 | 49 | 41 | 33 | 25 | 17 | 9 | 1 |
| 58 | 50 | 42 | 34 | 26 | 18 | 10 | 2 |
| 59 | 51 | 43 | 35 | 27 | 19 | 11 | 3 |
| 60 | 52 | 44 | 36 | 63 | 55 | 47 | 39 |
| 31 | 23 | 15 | 7 | 62 | 54 | 46 | 38 |
| 30 | 22 | 14 | 6 | 61 | 53 | 45 | 37 |
| 29 | 21 | 13 | 5 | 28 | 20 | 12 | 4 |

key after PC-1 → 1111 0000 1100 1100 1010 1010 0000 0000 1010 1100 1100 1111 0000 0000

here we halve the above bits and rotate left each half by one

key after rotation → 1110 0001 1001 1001 0101 0100 0001 0001 0101 1001 1001 1110 0000 0000



| PC − 2 | | | | | | | |
|---|---|---|---|---|---|---|---|
| 14 | 17 | 11 | 24 | 1 | 5 | 3 | 28 |
| 15 | 6 | 21 | 10 | 23 | 19 | 12 | 4 |
| 26 | 8 | 16 | 7 | 27 | 20 | 13 | 2 |
| 41 | 52 | 31 | 37 | 47 | 55 | 30 | 40 |
| 51 | 45 | 33 | 48 | 44 | 49 | 39 | 56 |
| 34 | 53 | 46 | 42 | 50 | 36 | 29 | 32 |

next using PC-2

result → 0000 1011 0000 0010 0110 0111 1001 1001 0100 1000 1010 0101

b. L0=0000 0001 0010 0011 0100 0101 0110 0111R0=1000 1001 1010 1011 1100 1101 1110 1111

c. E(R0)= 1100 0101 0011 1101 0101 0111 1110 0101 1011 1111 0101 1111

d. $E(R_0)\oplus k$=1100 1110 0011 1111 0011 0000 0111 1100 1111 0111 1111 1010

e. passing through s boxes → 1:1011 2:1000 3:1110 4:1111 5:0110 6:0101 7:0110 8:0011

f.10111000111011110110010101100011

g. applying permutation table → 1000 0000 1101 1111 0011 1111 1100 1110

h. R1→ 1000 0001 1111 1100 0111 1010 1010 1001

i. final ciphered text → 1000 1001 1010 1011 1100 1101 1110 1111 1000 0001 1111 1100 0111 1010 1010 1001

**4 :**

all of GF($2^4$) irreducible polynomials

$p(x) = a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$

since m=4 the $a_4$ should be 1 and if also $a_0$ should be 1 otherwise it'd be reducible.

for the rest of the coefficients $a_3 + a_2 + a_1 \neq 0$

final answer:

$$x^4 + x^3 + x^2 + x + 1$$

$$x^4 + x + 1$$

$$x^4 + x^3 + 1$$

**5.1 :**

ciphered text : j5a0edj2b

sample prefix text : WPI

palin text : WPIWOMBAT

**5.2 :**

initialization vector : 1,1,1,1,1,1

**5.3 :**

[1,1,0,0,0,0]

(0,1,6)

**5.4 :**

The common wombat lives mainly in wet, partly forested areas on the coast, and on the ranges and western slopes.

**5.5 :**

Known-plaintext Attack

** the python program is attached as 5_1_LFSR_decoding.py

**6 :**

like 1.3.7 since this key is a weak key, DES becomes a Feistel network and encryption becomes self-inverting so with twice DES encryption using this key we get the plain text itself.

**7 :**

a. text

| | | | |
|---|---|---|---|
| 00 | 04 | 08 | 0C |
| 01 | 05 | 09 | 0D |
| 02 | 06 | 0A | 0E |

|  |  |  |  |
|---|---|---|---|
| 03 | 07 | 0B | 0F |

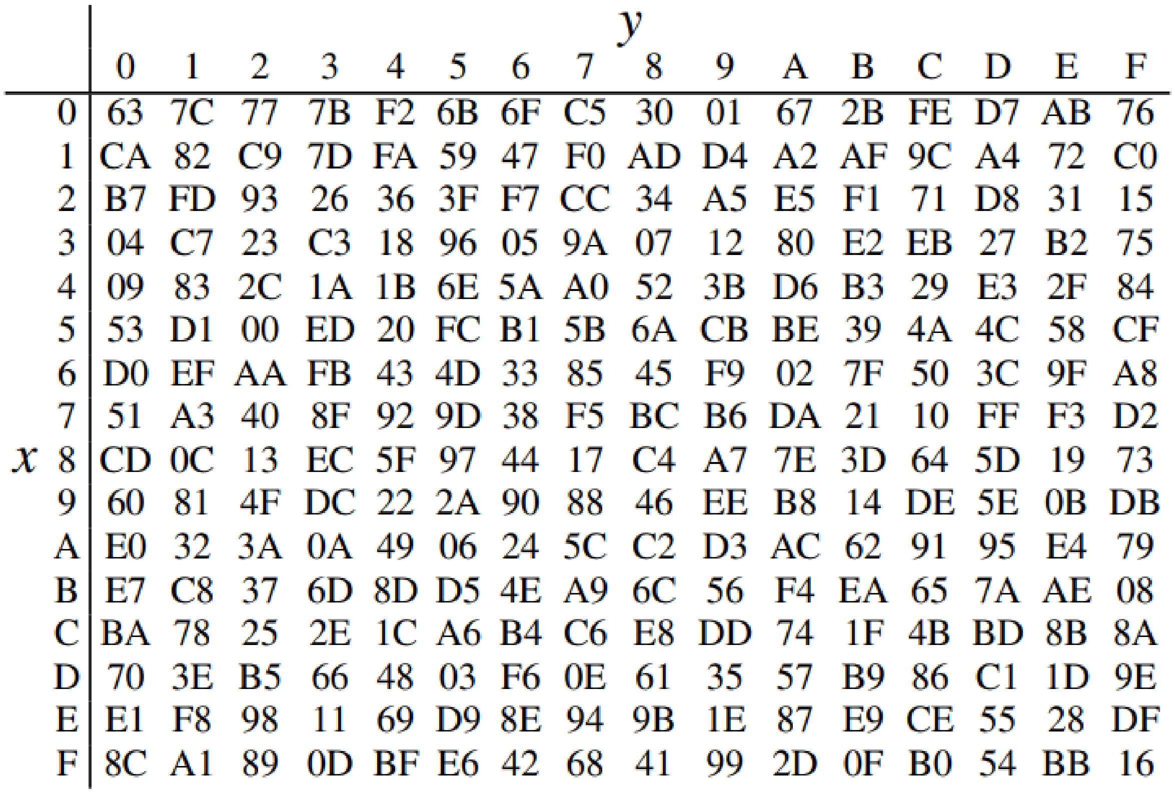
key

|  |  |  |  |
|---|---|---|---|
| 01 | 01 | 01 | 01 |
| 01 | 01 | 01 | 01 |
| 01 | 01 | 01 | 01 |
| 01 | 01 | 01 | 01 |

b.

|  |  |  |  |
|---|---|---|---|
| 01 | 05 | 09 | 0D |
| 00 | 04 | 08 | 0C |
| 03 | 07 | 0B | 0F |
| 02 | 06 | 0A | 0E |

c.

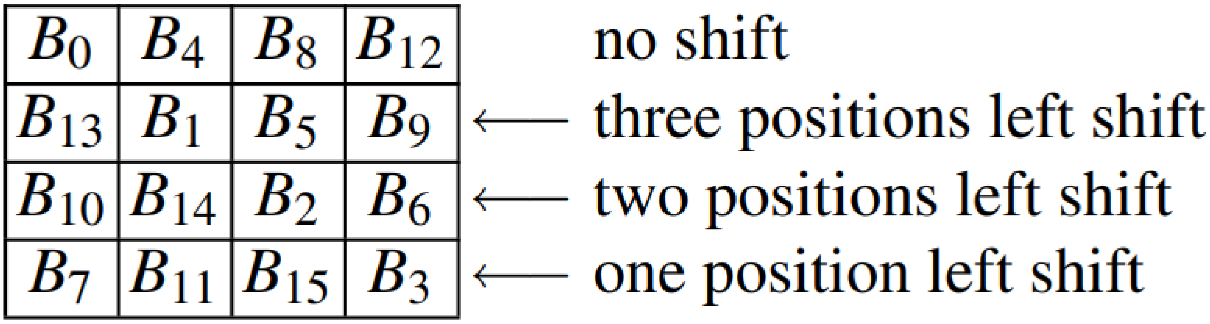


|  |  |  |  |  |  |  |  |  |  | *y* |  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
|  |  | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
|  | 0 | 63 | 7C | 77 | 7B | F2 | 6B | 6F | C5 | 30 | 01 | 67 | 2B | FE | D7 | AB | 76 |
|  | 1 | CA | 82 | C9 | 7D | FA | 59 | 47 | F0 | AD | D4 | A2 | AF | 9C | A4 | 72 | C0 |
|  | 2 | B7 | FD | 93 | 26 | 36 | 3F | F7 | CC | 34 | A5 | E5 | F1 | 71 | D8 | 31 | 15 |
|  | 3 | 04 | C7 | 23 | C3 | 18 | 96 | 05 | 9A | 07 | 12 | 80 | E2 | EB | 27 | B2 | 75 |
|  | 4 | 09 | 83 | 2C | 1A | 1B | 6E | 5A | A0 | 52 | 3B | D6 | B3 | 29 | E3 | 2F | 84 |
|  | 5 | 53 | D1 | 00 | ED | 20 | FC | B1 | 5B | 6A | CB | BE | 39 | 4A | 4C | 58 | CF |
|  | 6 | D0 | EF | AA | FB | 43 | 4D | 33 | 85 | 45 | F9 | 02 | 7F | 50 | 3C | 9F | A8 |
|  | 7 | 51 | A3 | 40 | 8F | 92 | 9D | 38 | F5 | BC | B6 | DA | 21 | 10 | FF | F3 | D2 |
| *x* | 8 | CD | 0C | 13 | EC | 5F | 97 | 44 | 17 | C4 | A7 | 7E | 3D | 64 | 5D | 19 | 73 |
|  | 9 | 60 | 81 | 4F | DC | 22 | 2A | 90 | 88 | 46 | EE | B8 | 14 | DE | 5E | 0B | DB |
|  | A | E0 | 32 | 3A | 0A | 49 | 06 | 24 | 5C | C2 | D3 | AC | 62 | 91 | 95 | E4 | 79 |
|  | B | E7 | C8 | 37 | 6D | 8D | D5 | 4E | A9 | 6C | 56 | F4 | EA | 65 | 7A | AE | 08 |
|  | C | BA | 78 | 25 | 2E | 1C | A6 | B4 | C6 | E8 | DD | 74 | 1F | 4B | BD | 8B | 8A |
|  | D | 70 | 3E | B5 | 66 | 48 | 03 | F6 | 0E | 61 | 35 | 57 | B9 | 86 | C1 | 1D | 9E |
|  | E | E1 | F8 | 98 | 11 | 69 | D9 | 8E | 94 | 9B | 1E | 87 | E9 | CE | 55 | 28 | DF |
|  | F | 8C | A1 | 89 | 0D | BF | E6 | 42 | 68 | 41 | 99 | 2D | 0F | B0 | 54 | BB | 16 |

|  |  |  |  |
|---|---|---|---|
| 7C | 6B | 01 | D7 |

| | | | |
|---|---|---|---|
| 63 | F2 | 30 | FE |
| 7B | C5 | 2B | 76 |
| 77 | 6F | 67 | AB |

d.



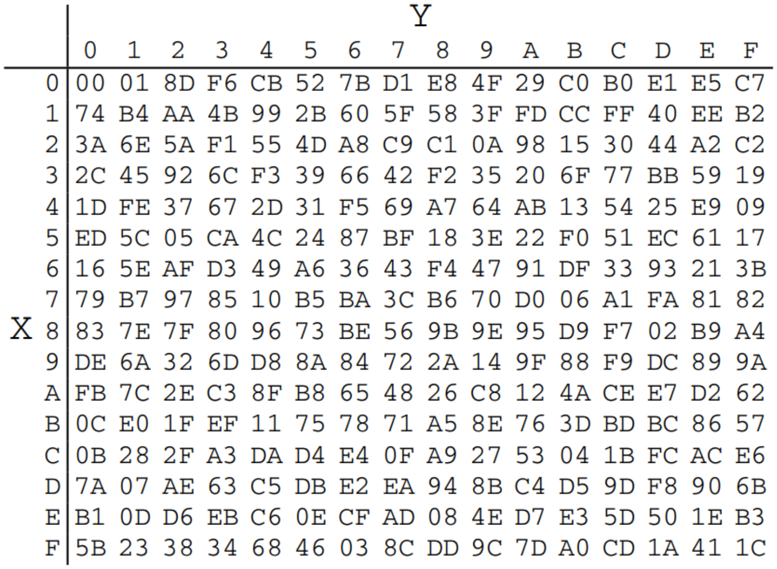
| | | | | |
|---|---|---|---|---|
| $B_0$ | $B_4$ | $B_8$ | $B_{12}$ | no shift |
| $B_{13}$ | $B_1$ | $B_5$ | $B_9$ | ⟵ three positions left shift |
| $B_{10}$ | $B_{14}$ | $B_2$ | $B_6$ | ⟵ two positions left shift |
| $B_7$ | $B_{11}$ | $B_{15}$ | $B_3$ | ⟵ one position left shift |

| | | | |
|---|---|---|---|
| 7C | 6B | 01 | D7 |
| F2 | 30 | FE | 63 |
| 2B | 76 | 7B | C5 |
| AB | 77 | 6F | 67 |

e.

$$\begin{pmatrix} C_0 \\ C_1 \\ C_2 \\ C_3 \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} B_0 \\ B_5 \\ B_{10} \\ B_{15} \end{pmatrix}$$

**Table 4.2** Multiplicative inverse table in $GF(2^8)$ for bytes *xy* used within the AES S-Box



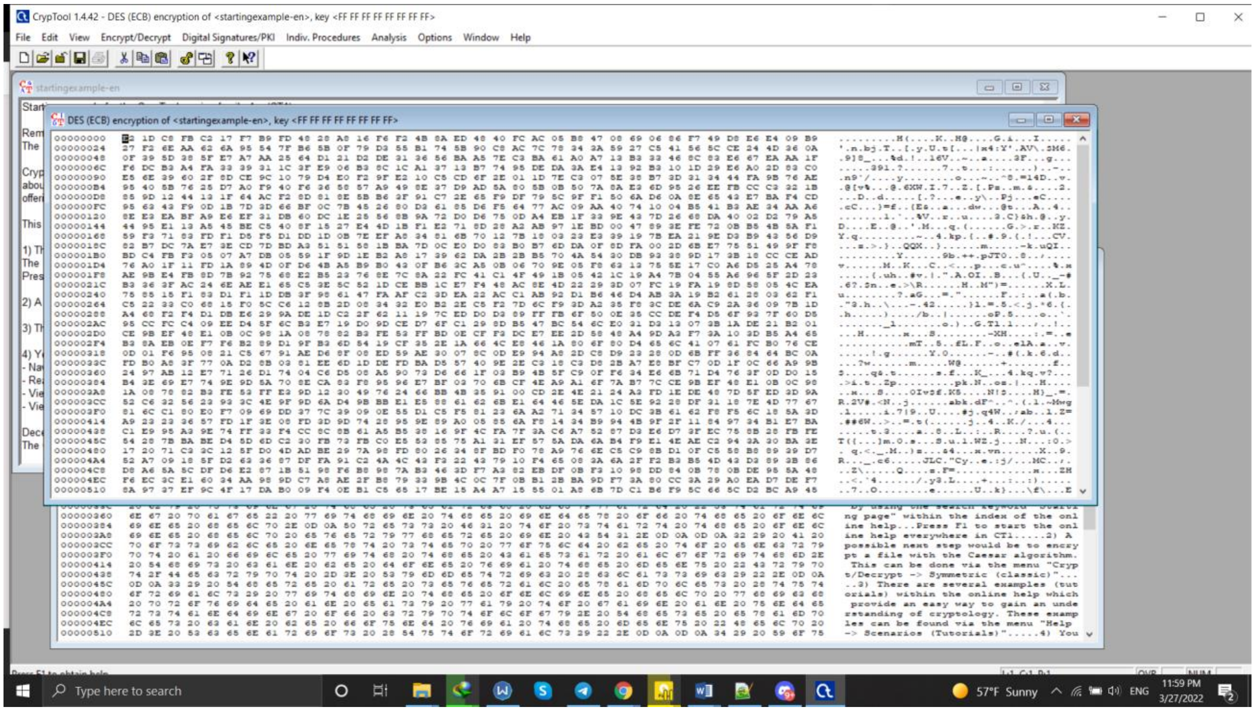
| | | | | | | | | | Y | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
| | 0 | 00 | 01 | 8D | F6 | CB | 52 | 7B | D1 | E8 | 4F | 29 | C0 | B0 | E1 | E5 | C7 |
| | 1 | 74 | B4 | AA | 4B | 99 | 2B | 60 | 5F | 58 | 3F | FD | CC | FF | 40 | EE | B2 |
| | 2 | 3A | 6E | 5A | F1 | 55 | 4D | A8 | C9 | C1 | 0A | 98 | 15 | 30 | 44 | A2 | C2 |
| | 3 | 2C | 45 | 92 | 6C | F3 | 39 | 66 | 42 | F2 | 35 | 20 | 6F | 77 | BB | 59 | 19 |
| | 4 | 1D | FE | 37 | 67 | 2D | 31 | F5 | 69 | A7 | 64 | AB | 13 | 54 | 25 | E9 | 09 |
| | 5 | ED | 5C | 05 | CA | 4C | 24 | 87 | BF | 18 | 3E | 22 | F0 | 51 | EC | 61 | 17 |
| | 6 | 16 | 5E | AF | D3 | 49 | A6 | 36 | 43 | F4 | 47 | 91 | DF | 33 | 93 | 21 | 3B |
| | 7 | 79 | B7 | 97 | 85 | 10 | B5 | BA | 3C | B6 | 70 | D0 | 06 | A1 | FA | 81 | 82 |
| X | 8 | 83 | 7E | 7F | 80 | 96 | 73 | BE | 56 | 9B | 9E | 95 | D9 | F7 | 02 | B9 | A4 |
| | 9 | DE | 6A | 32 | 6D | D8 | 8A | 84 | 72 | 2A | 14 | 9F | 88 | F9 | DC | 89 | 9A |
| | A | FB | 7C | 2E | C3 | 8F | B8 | 65 | 48 | 26 | C8 | 12 | 4A | CE | E7 | D2 | 62 |
| | B | 0C | E0 | 1F | EF | 11 | 75 | 78 | 71 | A5 | 8E | 76 | 3D | BD | BC | 86 | 57 |
| | C | 0B | 28 | 2F | A3 | DA | D4 | E4 | 0F | A9 | 27 | 53 | 04 | 1B | FC | AC | E6 |
| | D | 7A | 07 | AE | 63 | C5 | DB | E2 | EA | 94 | 8B | C4 | D5 | 9D | F8 | 90 | 6B |
| | E | B1 | 0D | D6 | EB | C6 | 0E | CF | AD | 08 | 4E | D7 | E3 | 5D | 50 | 1E | B3 |
| | F | 5B | 23 | 38 | 34 | 68 | 46 | 03 | 8C | DD | 9C | 7D | A0 | CD | 1A | 41 | 1C |

| | | | |
|---|---|---|---|
| A1 | DF | 01 | EA |
| 23 | 2C | 41 | D3 |
| 15 | BA | 06 | D4 |
| 4A | 77 | 3C | 43 |

**8.1 :**

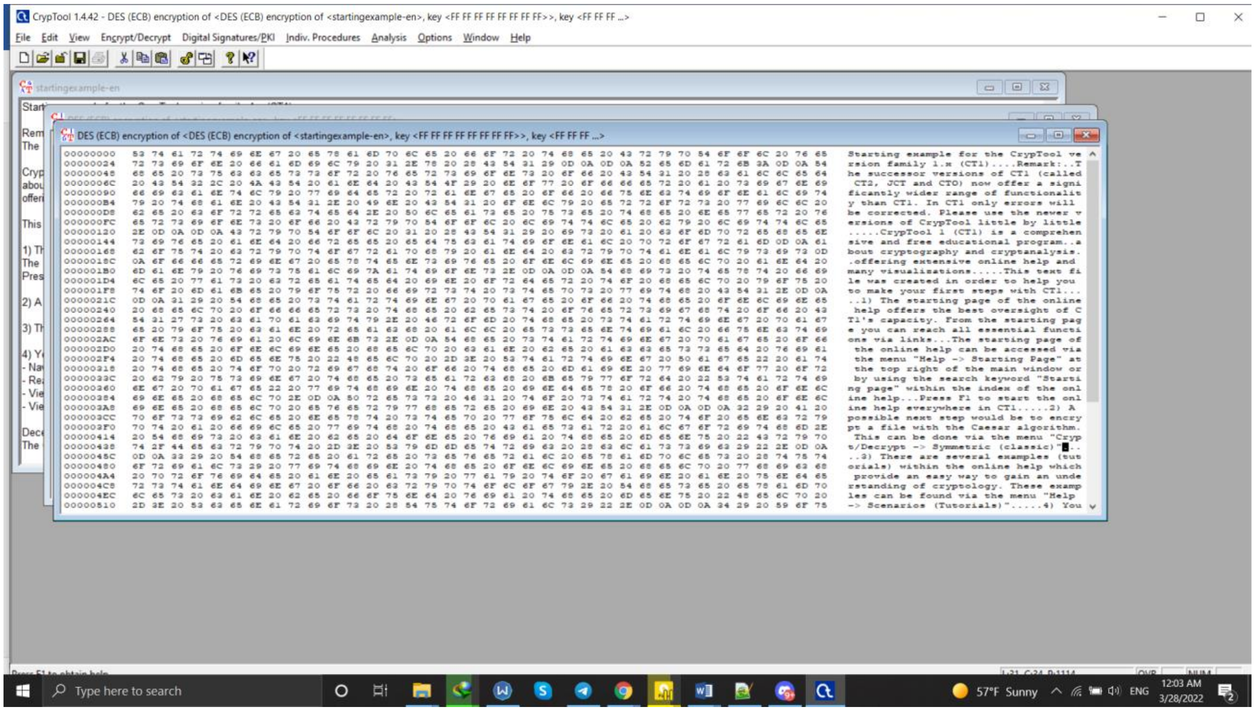
weak key : FF FF FF FF FF FF FF FF

first encryption



CrypTool 1.4.42 - DES (ECB) encryption of <startingexample-en>, key <FF FF FF FF FF FF FF FF>

second encryption



CrypTool 1.4.42 - DES (ECB) encryption of <DES (ECB) encryption of <startingexample-en>, key <FF FF FF FF FF FF FF FF>>, key <FF FF FF ...>

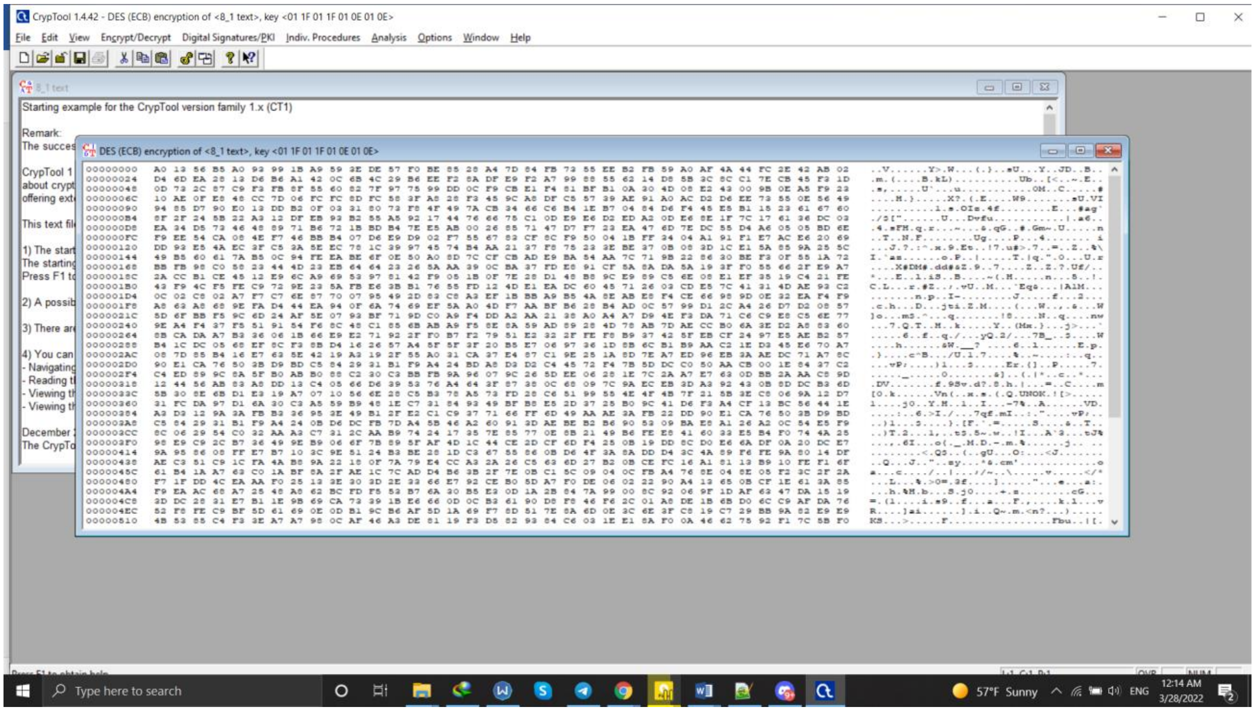
DES (ECB) encryption of <DES (ECB) encryption of <startingexample-en>, key <FF FF FF FF FF FF FF FF>>, key <FF FF FF ...>

```
Starting example for the CrypTool ve
rsion family 1.x (CT1)....Remark:..T
he successor versions of CT1 (called
 CT2, JCT and CTO) now offer a signi
ficantly wider range of functionalit
y than CT1. In CT1 only errors will 
be corrected. Please use the newer v
ersions of CrypTool little by little
.....CrypTool 1 (CT1) is a comprehen
sive and free educational program..a
bout cryptography and cryptanalysis.
.offering extensive online help and 
many visualizations.....This text fi
le 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 C
T1's capacity. From the starting pag
e you can reach all essential functi
ons 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 "Starti
ng page" within the index of the onl
ine help...Press F1 to start the onl
ine help everywhere in CT1.....2) A 
possible next step would be to encry
pt a file with the Caesar algorithm.
 This can be done via the menu "Cryp
t/Decrypt -> Symmetric (classic)"...
..3) There are several examples (tut
orials) within the online help which
 provide an easy way to gain an unde
rstanding of cryptology. These examp
les can be found via the menu "Help 
-> Scenarios (Tutorials)".....4) You
```

we observe that by encrypting twice we get the plaintext.

semi-weak key : 01 1F 01 1F 01 0E 01 0E

first encryption



CrypTool 1.4.42 - DES (ECB) encryption of <8_1 text>, key <01 1F 01 1F 01 0E 01 0E>

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

Remark:
The succes

CrypTool 1
about crypt
offering ext

This text fil

1) The start
The starting
Press F1 to

2) A possib

3) There are

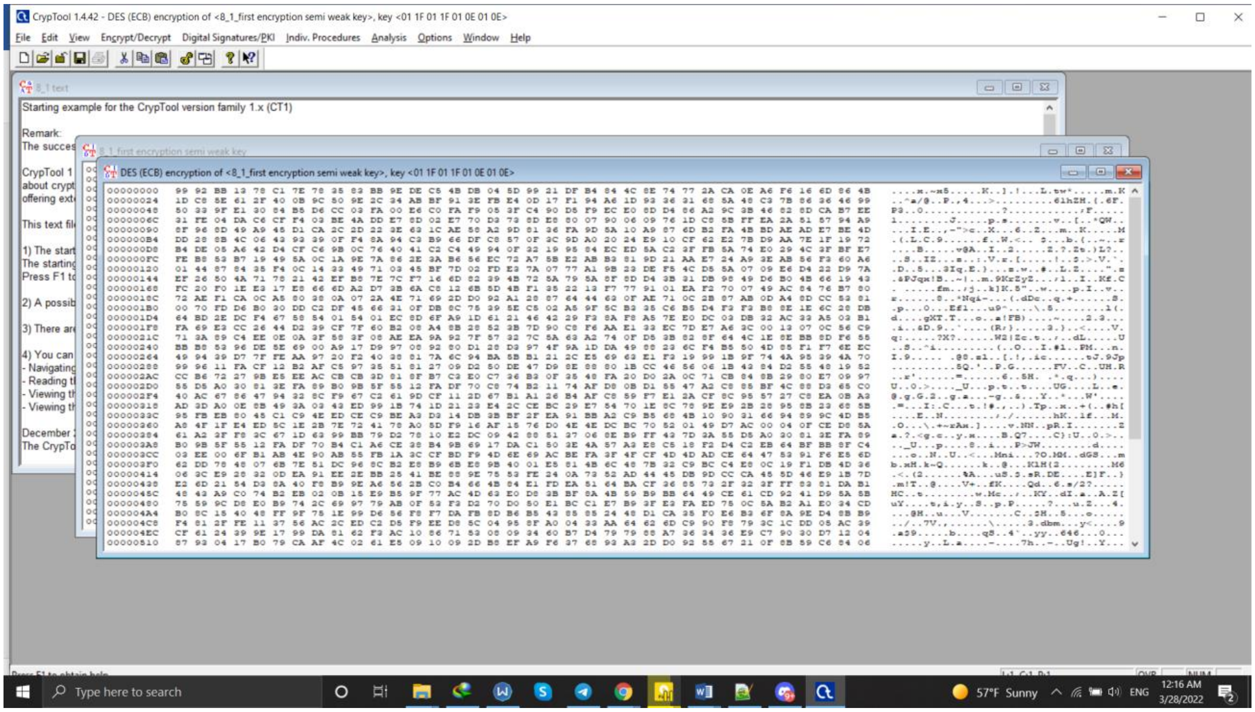
4) You can
- Navigating
- Reading t
- Viewing th
- Viewing th

December
The CrypTo

DES (ECB) encryption of <8_1 text>, key <01 1F 01 1F 01 0E 01 0E>

```
00000000  A0 13 56 B5 A0 93 99 1B A9 59 3E DE 57 F0 BE 85 28 A4 7D 84 FB 73 55 EE B2 FB 59 A0 AF 4A 44 FC 2E 42 AB 02  ..V.......Y>.W...(.}..sU...Y..JD..B..
00000024  D4 6D EA 28 13 D6 B6 A1 42 0C 6B 4C 29 B6 EE F2 8A DF E9 F2 A7 99 88 55 62 14 D8 5B 3C 8C C1 7E CB 45 F3 1D  .m.(....B.kL)...........Ub..[<..~.E..
00000048  0D 73 2C 87 C9 F3 FB 8F 55 60 82 7F 97 75 99 DD 0C F9 CB E1 F4 81 BF B1 0A 30 4D 08 E2 43 00 9B 0E A5 F9 23  .s,.....U`...u..............0M..C.....#
0000006C  10 AE 0F E8 48 CC 7D 06 FC FC 8D FC 58 3F A8 28 F3 45 9C A8 DF C5 57 39 AE 91 A0 AC D2 D6 EE 73 55 0E 56 49  ....H.}......X?.(.E....W9........sU.VI
00000090  94 85 D7 90 E0 13 DD B2 0F 03 31 80 73 F8 4F 49 7A CB 34 66 C6 B4 1E B7 04 84 D6 F4 45 E5 B1 15 23 61 67 60  ...........1.s.OIz.4f.........E...#ag`
000000B4  8F 2F 24 5B 22 A3 12 DF EB 93 B2 55 A5 92 17 44 76 66 75 C1 0D E9 E6 D2 ED A2 0D E6 8E 1F 7C 17 61 36 DC 03  ./$["......U...Dvfu.............|.a6..
000000D8  EA 34 D5 73 46 48 89 71 B6 72 1B BD B4 7E E5 AB 00 26 85 71 47 D7 F7 23 EA 47 6D 7E DC 55 D4 A6 05 05 BD 6E  .4.sFH.q.r...~...&.qG..#.Gm~.U......n
000000FC  F9 EE 54 CA 08 4E F7 46 BB B4 07 D6 E9 D9 02 F7 55 67 83 CF 8C F9 50 04 1B FF 34 04 A1 91 F1 E7 AC E6 20 69  ..T..N.F........Ug....P...4........ i
00000120  DD 93 E5 4A EC 3F C5 3A 5E EC 78 1C 39 97 45 74 B4 AA 21 37 F8 75 23 3E BE 37 0B 08 3D 1C E1 5A 85 9A 25 5C  ...J.?.:^.x.9.Et..!7.u#>.7..=..Z..%\
00000144  49 B5 60 61 7A B5 0C 94 FE EA BE 6F 0E 50 A0 8D 7C CF CB AD E9 BA 54 AA 7C 71 9B 22 86 30 BE F3 0F 55 1A 72  I.`az.......o.P..|.....T.|q.".0...U.r
00000168  BB FB 98 C0 58 23 44 4D 23 EB 64 64 23 26 5A AA 39 0C BA 37 FD E8 91 CF 8A 8A DA 5A 19 3F F0 55 66 2F E9 A7  ....X#DM#.dd#&Z.9..7.....Z..Z.?.Uf/..
0000018C  2A CC B1 CE 45 12 E9 6C A9 69 53 97 81 42 F9 05 1B 0F 7E 28 D1 48 B8 9C E9 89 C5 6E 08 E1 EF 35 19 C4 21 FE  *...E..l.iS..B....~(.H.....n...5..!.
000001B0  43 F9 4C F5 FE C9 72 9E 23 5A FB E6 3B B1 76 55 FD 12 4D E1 EA DC 60 45 71 26 03 CD E5 7C 41 31 4D AE 93 C2  C.L...r.#Z..;.vU..M...`Eq&...|A1M...
000001D4  0C 02 C8 02 A7 F7 C7 6E 87 70 07 95 49 2D 83 C8 A3 EF 1B BB A9 B5 4A 8E AB E8 F4 CE 66 98 9D 0E 32 EA F4 F9  .......n.p..I-........J.....f...2...
000001F8  A8 63 A8 68 9E FA D4 44 EA 94 0F 6A 74 69 EF 5A A0 4D F7 AA BF B6 28 B4 AD 0C 57 99 D1 2C A4 26 D7 D2 08 57  .c.h...D...jti.Z.M.....(...W..,.&...W
0000021C  5D 6F BB F5 9C 6D 24 AF 5E 07 93 BF 71 9D C0 A9 F4 DD A2 AA 21 38 A0 A4 A7 D9 4E F3 DA 71 C6 C9 E8 C5 6E 77  ]o...m$.^...q.......!8....N..q....nw
00000240  9E A4 F4 37 F5 51 91 54 F6 8C 48 C1 85 6B AB A9 F5 8E 8A 59 AD 89 28 4D 78 AB 7D AE CC B0 6A 3E D2 A8 83 60  ...7.Q.T..H..k.....Y..(Mx.}...j>...`
00000264  8B CA DA A7 B3 36 06 1B 66 E9 E2 71 92 2F F0 B7 F2 79 51 E2 32 2F FE F8 B9 37 42 5F EB CF 24 97 E5 AE B2 57  .....6..f..q./...yQ.2/...7B_..$....W
00000288  B4 1C DC 05 68 EF 8C F3 8B D4 16 26 57 A4 5F 5F 3F 20 B5 E7 06 97 36 1D 8B 6C B1 B9 AA C2 1E D3 45 E6 70 A7  ....h......&W.__? ....6..l......E.p.
000002AC  08 7D 85 B4 16 E7 63 5E 42 19 A3 19 2F 55 A0 31 CA 37 E4 87 C1 9E 25 1A 8D 7E A7 ED 96 EB 3A AE DC 71 A7 8C  .}....c^B.../U.1.7....%..~....:..q..
000002D0  90 E1 CA 76 50 3B D9 BD C5 84 29 31 B1 F9 A4 24 BD A8 D3 D2 C4 45 72 F4 7B 5D DC C0 50 AA CB 00 1E 84 37 C2  ...vP;....)1...$.....Er.{]..P.....7.
000002F4  C4 ED 89 9C 8A 5F B0 AB B0 88 C2 30 C3 BB FB 9A 96 07 9C 26 5D EE 06 28 1E 7C 2A A7 E7 63 0D BB 2A AA C8 9D  ....._.....0.......&]..(.|*..c..*...
00000318  12 44 56 AB 83 A8 DD 13 C4 05 66 D6 39 53 76 A4 64 3F 87 38 0C 68 09 7C 9A EC EB 3D A3 92 43 0B 8D DC B3 6D  .DV.......f.9Sv.d?.8.h.|...=..C....m
0000033C  5B 30 8E 6B D1 E3 19 A7 07 10 56 6E 28 C5 B3 78 A5 73 FD 28 C6 51 99 55 4E 4F 4B 7F 21 5B 3E C8 06 9A 12 D7  [0.k......Vn(..x.s.(.Q.UNOK.![>.....
00000360  31 FC DA 97 D1 6A 30 C3 A5 59 B9 48 1E C7 31 84 93 49 BF B8 E5 2D 37 25 B0 9C 41 D6 F3 A4 CF 13 BC 56 44 1E  1....j0..Y.H..1..I...-7%..A......VD.
00000384  A3 D3 12 9A 3A FB B3 36 95 3E 49 B1 2F E2 C1 C9 37 71 66 FF 6D 49 AA AE 3A FB 22 DD 90 E1 CA 76 50 3B D9 BD  ....:..6.>I./...7qf.mI..:."....vP;..
000003A8  C5 84 29 31 B1 F9 A4 24 0B D6 DC FB 7D A4 5B 46 A2 60 91 3D AE BE B2 B6 90 53 09 BA E8 A1 26 A2 0C 54 E5 F9  ..)1...$....}.[F.`.=.....S....&..T..
000003CC  8C 06 29 54 C0 32 AA A3 C7 31 2C AA B9 74 24 17 35 7E 85 77 0E 8B 21 49 B6 FE E8 41 60 33 E5 B4 F0 74 4A 25  ..)T.2...1,..t$.5~.w..!I...A`3...tJ%
000003F0  98 E9 C9 2C B7 36 49 9E B9 06 6F 7B 89 5F AF 4D 1C 44 CE 2D CF 6D F4 25 0B 19 DD 8C D0 E6 6A DF 0A 20 DC E7  ...,.6I...o{._.M.D.-.m.%......j.. ..
00000414  9A 95 86 08 FF E7 B7 10 3C 9E 51 24 B3 BE 28 1D C3 67 58 86 0B D6 4F 3A 8A DD D4 3C 4A 89 F6 FE 9A 80 14 DF  ........<.Q$..(..gX...O:...<J.......
00000438  AE C3 51 C9 1C FA 4A B8 9A 22 18 0F 7A 79 E4 CC A3 2A 26 C5 63 6D 27 B2 0B CE FC 16 A1 81 13 B9 10 FE F1 6F  ..Q...J..."..zy...*&.cm'............o
0000045C  61 B4 1A A7 63 C0 1A BF 8A 2F AE 1C 7C AD D4 B6 3B 2F 7E 0B C1 5C 09 04 0C FB A4 76 8E 04 8E 05 F2 3C 2F 2A  a...c..../..|...;/~..\.....v.....</*
00000480  F7 1F DD 4C EA AA F0 25 13 3E 30 3D 2E 33 66 E7 92 CE B0 5D A7 F0 DE 06 02 22 90 A4 13 65 0B CF 1E 61 3A 85  ...L...%.>0=.3f....].....".. .e...a:.
000004A4  F9 EA AC 68 A7 25 48 A8 62 BC FD F5 53 B7 6A 30 B5 E3 0D 1A 2B 84 7A 99 00 8C 92 06 9F 1D AF 63 47 DA 15 19  ...h.%H.b...S.j0....+.z..........cG...
000004C8  3D DC 28 31 E7 B1 1E 9B 69 CA 73 39 1B E6 66 0D 0C B3 61 90 D8 F8 46 F6 2C 01 A8 DE 1B 6B D0 6C C9 AF DA 76  =.(1....i.s9..f...a...F.,....k.l....v
000004EC  52 F8 FE C9 BF 5D 61 69 0E 0D B1 9C B6 AF 5D 1A 69 F7 8D 51 7E 8A 6D 0E 3C 6E 3F C8 19 C7 29 BB 9A 82 E9 E9  R....]ai......].i..Q~.m.<n?...)......
00000510  4B 53 85 C4 F3 3E A7 A7 98 0C AF 46 A3 DE 81 19 F3 D5 82 93 84 C6 03 1E E1 8A F0 0A 46 62 78 92 F1 7C 5B F0  KS...>.....F...................Fbx..|[.
```

second encryption


CrypTool 1.4.42 - DES (ECB) encryption of <8_1_first encryption semi weak key>, key <01 1F 01 1F 01 0E 01 0E>
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
8_1 text
8_1_first encryption semi weak key
DES (ECB) encryption of <8_1_first encryption semi weak key>, key <01 1F 01 1F 01 0E 01 0E>
Type here to search
57°F Sunny
ENG
12:16 AM
3/28/2022

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

Remark:
The succes

CrypTool 1
about crypt
offering ext

This text fil

1) The start
The starting
Press F1 to

2) A possib

3) There are

4) You can
- Navigating
- Reading tl
- Viewing th
- Viewing th

December
The CrypTo

```
00000000   99 92 BB 13 78 C1 7E 78 35 83 BB 9E DE C5 4B DB 04 5D 99 21 DF B4 84 4C 8E 74 77 2A CA 0E A6 F6 16 6D 86 4B   ....x.~x5.....K..].!...L.tw*.....m.K
00000024   1D C8 5E 61 2F 40 0B 9C 50 9E 2C 34 AB BF 91 3E FB E4 0D 17 F1 94 A6 1D 93 36 31 68 5A 48 C3 7B 86 36 46 99   ..^a/@..P.,4...>.........61hZH.{.6F.
00000048   50 33 9F E1 30 84 B5 D6 CC 03 FA 00 E6 C0 FA F9 05 3F C4 90 D5 F9 EC E0 8D D4 86 A2 9C 3B 46 82 8D CA B7 EE   P3..0............?...........;F.....
0000006C   31 FE 04 DA C6 CF F4 03 BE 4A DD E7 8D 02 E7 70 D3 73 8D E8 80 07 90 06 09 76 1D C8 5B FF EA 2A 51 57 94 A9   1.........J.....p.s........v..[..*QW..
00000090   8F 96 8D 49 A9 45 D1 CA 2C 2D 22 3E 63 1C AE 58 A2 9D 81 36 FA 9D 5A 10 A9 87 6D B2 FA 4B BD AE AD E7 BE 4D   ...I.E..,-">c..X...6..Z...m..K.....M
000000B4   DD 28 8B 4C 06 43 93 39 0F F4 8A 94 C3 B9 66 DF C8 57 0F 3C 9D A0 20 24 E9 10 CF 62 E2 7B D9 AA 7E 1F 19 72   .(.L.C.9......f..W.<.. $...b.{..~..r
000000D8   B4 DE 05 A6 42 D4 CF C6 9B 0C 76 40 41 C2 C4 49 94 0F 32 19 95 84 EC ED 5A C2 3F FB 5A 74 E0 29 4C 3F BF E7   ....B.....v@A..I..2.....Z.?.Zt.)L?..
000000FC   FE B8 53 B7 19 49 5A 0C 1A 9E 7A 86 2E 3A B6 56 EC 72 A7 5B E2 AB B3 81 9D 21 AA E7 24 A9 3E AB 56 F3 60 A6   ..S..IZ...z..:.V.r.[.....!..$.>.V.`.
00000120   01 44 87 84 35 F4 0C 14 33 49 71 03 45 BF 7D 02 FD E3 7A 07 77 A1 9B 23 DE F5 4C D5 5A 07 09 E6 D4 22 D9 7A   .D..5...3Iq.E.}...z.w..#..L.Z....".z
00000144   EF 26 50 4A 71 78 21 42 EF B8 7E 7C F7 16 6D 82 39 4B 72 5A 79 5A 8F 8D D4 3B 31 DB 98 49 D6 B0 4B 66 19 43   .&PJqx!B..~|..m.9KrZyZ...;1..I..Kf.C
00000168   FC 20 F0 1E E3 17 E8 66 6D A2 D7 3B 6A C8 12 6B 5D 4B F1 35 22 13 F7 77 91 01 EA F2 70 07 49 AC 84 76 B7 80   . .....fm..;j..k]K.5"..w....p.I..v..
0000018C   72 AE F1 CA 0C A5 80 38 0A 07 2A 4E 71 69 2D D0 92 A1 28 87 64 44 63 0F AE 71 0C 2B 87 AB 0D A4 8D CC 53 81   r......8..*Nqi-...(.dDc..q.+......S.
000001B0   00 70 FD D6 B0 30 DD C2 DF 45 66 31 0F DB 8C 75 39 5E C5 02 A5 9F 5C B3 35 C6 B5 D4 F3 F3 B8 8E 1E 6C 28 DB   .p...0...Ef1...u9^....\.5........l(.
000001D4   64 BD 2E DC F4 67 58 54 01 54 01 EC 8D 6F A9 1D 61 21 46 42 29 F3 8A F8 A5 7E E0 DC 03 DB 32 AC 33 A5 03 B1   d....gXT.T...o..a!FB)....~....2.3...
000001F8   FA 69 E3 CC 26 44 D2 39 CF 7F 60 B2 08 A4 8B 28 52 3B 7D 90 C8 F6 AA E1 33 EC 7D E7 A6 3C 00 13 07 0C 56 C9   .i..&D.9..`....(R;}.....3.}..<....V.
0000021C   71 3A 89 C4 EE 0E 0A 3F 58 3F 08 AE EA 9A 92 7F 57 32 7C 5A 63 A2 74 0F D5 3B 82 8F 64 4C 1E 8E BB 8D F6 55   q:.....?X?......W2|Zc.t..;..dL.....U
00000240   BB B8 53 96 DE 5E 69 00 A9 17 D9 97 08 92 80 D1 28 D3 97 4F 9A 1D DA 49 88 23 6C F4 B5 50 4D 85 F1 F7 6E EC   ..S..^i.........(..O...I.#l..PM...n.
00000264   49 94 39 D7 7F FE AA 97 20 F2 40 38 81 7A 6C 94 BA 5B B1 21 2C E5 69 63 E1 F3 19 99 1B 9F 74 4A 95 39 4A 70   I.9..... .@8.zl..[.!,.ic......tJ.9Jp
00000288   99 96 11 FA CF 12 B2 AF C5 97 35 51 81 27 09 D2 50 DE 47 D9 8E 88 80 1B CC 46 56 06 1B 43 84 D2 55 48 19 52   ..........5Q.'..P.G......FV..C..UH.R
000002AC   CC B6 72 27 9B E5 EE AC CB CB 3D 81 8F B7 C3 E0 C7 36 B3 0F 35 48 FA 20 D0 2A 0C 71 CB 84 8B 29 80 E7 09 97   ..r'......=......6..5H. .*.q...)....
000002D0   55 D5 A0 30 81 3E FA 89 B0 9B 5F 55 12 FA DF 70 C8 74 B2 11 74 AF D8 0B D1 85 47 A2 C8 85 BF 4C 88 D3 65 C0   U..0.>...._U...p.t..t....UG....L..e.
000002F4   40 AC 67 86 47 94 32 8C F9 67 C2 61 9D CF 11 2D 67 B1 A1 26 B4 AF C8 59 F7 E1 2A CF 8C 95 57 27 C8 EA 0B A3   @.g.G.2..g.a...-g..&...Y..*...W'....
00000318   AD 3D A0 0E 8B 49 3A 03 43 ED 99 1B 74 1D 21 23 E4 2C CE BC 29 E7 54 70 1E 8C 78 9E E9 2B 28 95 8B 23 68 5B   .=...I:.C...t.!#.,..).Tp..x..+(..#h[
0000033C   95 FB EB 80 45 C1 C9 4E ED CE C9 BE A3 D3 14 DB 3B BF 2F EA 91 BB A2 C9 B5 68 4B 10 90 31 66 94 89 9C 4D B5   ....E..N........;./......hK..1f...M.
00000360   A8 4F 1F E4 ED 5C 1E 2B 7E 72 41 78 A0 5D F9 16 AF 15 76 D0 4E 4E DC BC 70 52 01 49 D7 AC 00 04 0F CE D8 5A   .O...\.+~rAx.]....v.NN..pR.I.......Z
00000384   61 A2 3F F8 3C 67 1D 63 99 BB 79 D2 78 10 E2 DC 09 42 88 51 37 06 8E B9 FF 43 7D 3A 55 D5 A0 30 81 3E FA 89   a.?.<g.c..y.x....B.Q7....C}:U..0.>..
000003A8   B0 9B 5F 55 12 FA DF 70 B4 C1 A6 CE 38 B4 9B 69 17 DA C1 50 3E 4A 57 A3 E8 C5 18 F2 D4 C2 EB 64 BF BB 8F C4   .._U...p....8..i...P>JW.........d....
000003CC   03 EE 00 6F B1 AB 4E 90 AB 55 FB 1A 3C CF BD F9 4D 6E 69 AC BE FA 3F 4F CF 4D 4D AD CE 64 47 53 91 F6 E5 6D   ...o..N..U..<...Mni...?O.MM..dGS...m
000003F0   62 DD 78 48 07 6B 7E 51 DC 96 8C B2 E8 B9 6B E8 9B 40 01 E5 81 4B 6C 48 7B 32 C9 BC C4 E8 0C 19 F1 DB 4D 36   b.xH.k~Q......k..@...KlH{2........M6
00000414   06 3C E9 28 32 0D EA 91 EE 2E BB 25 41 BE 88 9E 75 53 FE 24 0A 73 52 AD 44 45 DB 9D CC CA 45 5D 46 E9 1B 7D   .<.(2......%A...uS.$.sR.DE....E]F..}
00000438   E2 6D 21 54 D3 8A 40 F8 B9 9E A6 56 2B C0 B4 66 4B 84 E1 FD EA 51 64 BA CF 36 85 73 2F 32 3F FF 83 81 DA B1   .m!T..@....V+..fK....Qd..6.s/2?.....
0000045C   48 43 A9 C0 74 B2 EB 02 0B 15 E9 B5 9F 77 AC 4D 63 E0 D8 3B BF 8A 4B 59 B9 BB 64 49 CE 61 CD 92 41 D9 5A 5B   HC..t.........w.Mc..;..KY..dI.a..A.Z[
00000480   75 59 9C D8 E0 B9 74 2C 69 97 79 AB 0F 53 F3 D2 70 D0 50 E1 BC C1 E7 B9 3F E3 FA ED 75 0C 5A B2 A1 E0 34 CD   uY....t,i.y..S..p.P.....?...u.Z...4.
000004A4   B0 8C 15 40 48 FF 9F 75 1E 99 D6 56 F8 F7 DA FB 8D B6 B5 43 85 85 24 48 D1 CA 35 F0 E6 B3 6F 8A 9E D4 8B B9   ...@H..u...V.......C..$H..5...o.....
000004C8   F4 81 2F FE 11 37 56 AC 2C ED C2 D5 F9 EE D8 5C 04 95 8F A0 04 33 AA 64 62 6D C9 90 F8 79 3C 1C DD 05 AC 39   ../..7V.,......\.....3.dbm...y<....9
000004EC   CF 61 24 39 9E 17 99 DA 81 62 F3 AC 10 86 71 53 08 09 34 60 B7 D4 79 79 88 A7 36 34 36 E9 C7 90 30 D7 12 04   .a$9.....b....qS..4`..yy..646...0...
00000510   87 93 04 17 B0 79 CA AF 4C 02 61 E5 09 10 09 2D B8 EF A9 F6 37 68 93 A3 2D D0 92 55 67 21 0F 8B 59 C6 84 06   .....y..L.a....-....7h..-..Ug!..Y...
```

## 8.2 :

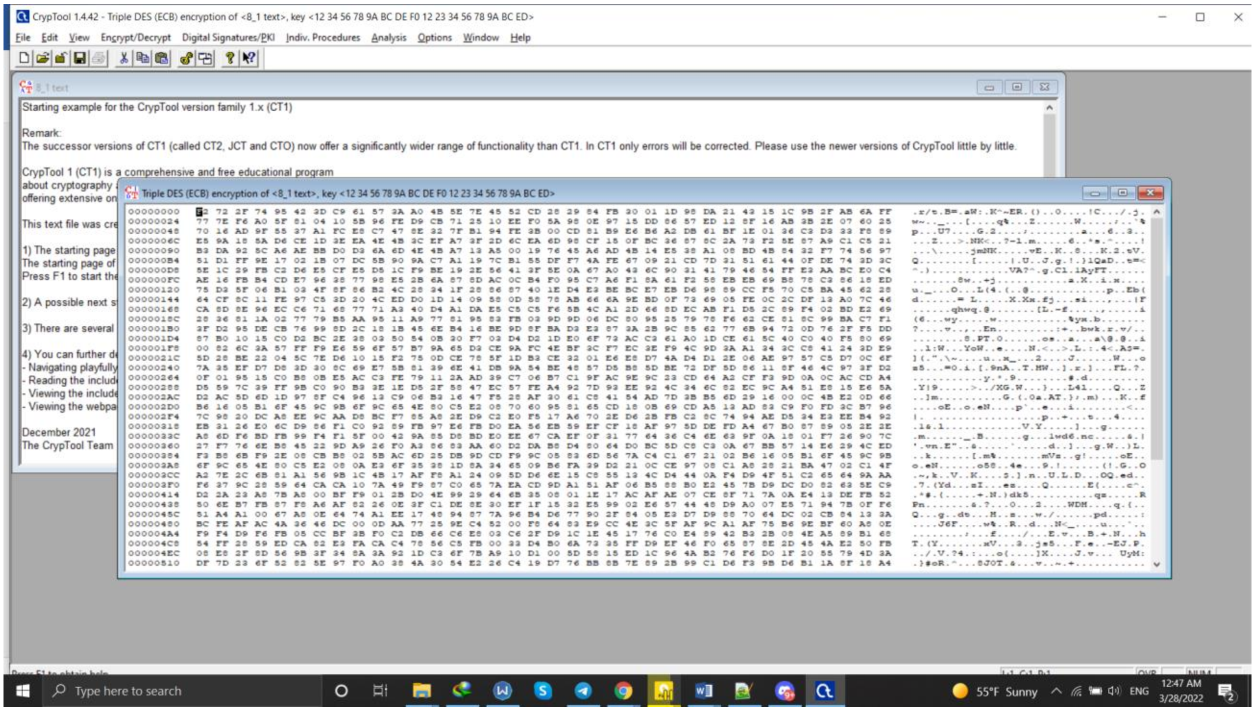
i. because it uses three different keys so the search space for the key get increased by a factor of 2 in power.

ii. mentioned in the previous part the reason is a type of attack called meet in the middle which causes us to always get coefficient of key length reduced by 1.

iii. one version does encryption – decryption – encryption and the other one does decryption – encryption – decryption.

if all the keys being independent for brute force attack the power of two is 2*k but if first and third keys are identical then its only k.

iv. key 12 34 56 78 9A BC DE F0 12 23 34 56 78 9A BC ED



CrypTool 1.4.42 - Triple DES (ECB) encryption of <8_1 text>, key <12 34 56 78 9A BC DE F0 12 23 34 56 78 9A BC ED>

File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help

8_1 text

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
offering extensive on

This text file was cre

1) The starting page
The starting page of
Press F1 to start the

2) A possible next s

3) There are several

4) You can further d
- Navigating playfully
- Reading the includ
- Viewing the include
- Viewing the webpa

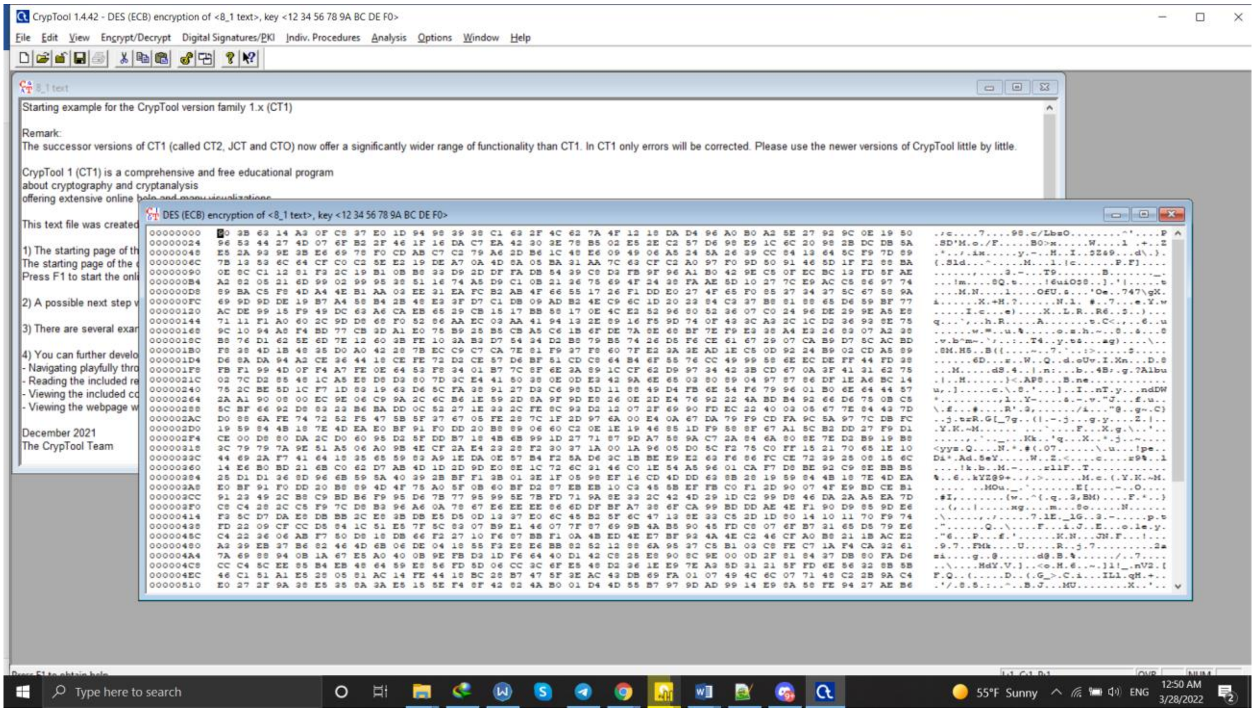
December 2021
The CrypTool Team

Triple DES (ECB) encryption of <8_1 text>, key <12 34 56 78 9A BC DE F0 12 23 34 56 78 9A BC ED>

```
00000000  E2 72 2F 74 95 42 3D C9 61 57 3A A0 4B 5E 7E 45 52 CD 28 29 84 FB 30 01 1D 98 DA 21 43 15 1C 9B 2F AB 6A FF
00000024  77 7E F6 A0 5F 81 04 10 5B 96 FE D9 CB 71 25 10 EE F0 5A 98 0E 97 15 DD 86 57 ED 12 8F 16 AB 3B 2E 07 60 25
00000048  70 16 AD 9F 55 37 A1 FC E8 C7 47 8E 32 7F B1 94 FE 3B 00 CD 81 B9 E6 B6 A2 DB 61 BF 1E 01 36 C3 D3 33 F8 89
0000006C  E5 9A 18 5A D6 CE 1D 3E EA 4E 4B 3C EF A7 3F 2D 6C EA 6D 98 CF 18 0F BC 36 87 8C 2A 73 F2 8E 87 A9 C1 C5 21
00000090  B3 DA 92 8C A6 AE BB D0 D3 6A 6D 4E 4B A7 13 A5 00 19 76 45 A6 AD 4B 14 E5 38 A1 08 BD 4B 84 32 F7 74 86 97
000000B4  51 D1 FF 9E 17 02 1B 07 DC 5B 90 9A C7 A1 19 7C B1 55 DF F7 4A FE 67 09 21 CD 7D 31 51 61 44 0F DE 74 3D 3C
000000D8  5E 1C 29 FB C2 D6 E5 CF E5 D5 1C F9 BE 19 2E 56 41 3F 8E 0A 67 A0 43 6C 90 31 41 79 46 54 FF E3 AA BC E0 C4
000000FC  AE 16 FB B4 CD E7 96 38 77 98 E5 2B 6A 87 8D AC 0C B4 F0 95 C7 A6 F1 8A 61 F2 58 EB EB 69 B8 78 C3 86 18 ED
00000120  75 D3 5F 06 B1 03 4F 8F 86 B2 4C 28 34 1F 28 86 87 40 1E D4 E3 BE BC E7 EB D6 98 89 CC F5 70 C5 BA 45 62 28
00000144  64 CF 8C 11 FE 97 C5 3D 20 4C ED D0 1D 14 09 58 0D 58 78 AB 66 6A 9E BD 0F 73 69 05 FE 0C 2C DF 13 A0 7C 46
00000168  CA 8D 8E 96 EC C6 71 68 77 71 A3 40 D4 A1 DA E5 C5 C5 F6 5B 4C A1 2D 66 8D EC AB F1 D5 2C 89 F4 02 BD E2 69
0000018C  28 36 81 1A 02 77 79 B5 AA 95 11 A9 77 81 95 83 FB 03 9D 9D 06 DC 80 95 25 79 78 F6 62 CE 81 8C 99 BA C7 F1
000001B0  3F D2 95 DE CB 76 99 8D 2C 18 1B 45 6E B4 16 BE 9D 8F BA D3 E3 87 3A 2B 9C 85 62 77 6B 94 72 0D 76 2F F5 DD
000001D4  87 B0 10 15 C0 D2 BC 2E 38 03 50 54 0B 30 F7 03 D4 D2 1D E0 6F 73 AC C3 61 A0 1D CE 61 5C 40 C0 40 F5 80 69
000001F8  00 82 6C 3A 57 FF F9 E6 59 6F 57 B7 9A 65 D3 CE 9A FC 4E BF 3C F7 EC 3E F9 4C 9D 3A A1 34 3C C8 41 24 3D E9
0000021C  5D 28 BE 22 04 5C 7E D6 10 15 F2 75 0D CE 78 5F 1D B3 CE 32 01 E6 E8 D7 4A D4 D1 2E 06 AE 97 57 C5 D7 0C 6F
00000240  7A 35 EF D7 D8 3D 30 8C 69 E7 5B 81 39 6E 41 DB 9A 54 BE 48 57 D5 B8 5D BE 72 DF 5D 86 11 8F 46 4C 97 3F D2
00000264  0F 01 95 15 C0 B8 0B E5 AC C3 FE 79 11 2A AD 39 C7 06 B7 C1 9F AC 9E 9C 23 CD 64 A2 CF F3 9D 0A 0C AC CD A4
00000288  D5 59 7C 39 FF 9B C0 90 B3 3E 1E D5 2F 58 47 EC 57 FE A4 92 7D 93 EE 92 4C 34 6C 82 EC 9C A4 51 E8 15 E6 5A
000002AC  D2 AC 5D 6D 1D 97 8F C4 96 13 C9 06 B3 16 47 F5 28 AF 30 61 C8 41 54 AD 7D 3B B5 6D 29 16 00 0C 4B E2 0D 66
000002D0  B6 16 05 B1 6F 45 9C 9B 6F 9C 65 4E 80 C5 E2 08 70 60 95 81 65 CD 18 0B 69 CD A5 13 AD 83 C9 F0 FD 3C B7 96
000002F4  7C 98 20 DC A8 EE 9C AA D8 BC F7 85 A8 2E D9 C2 E0 F5 17 A6 70 2E D6 2B FB C2 8C 74 94 AE D5 34 E3 EE B4 92
00000318  EB 31 26 E0 6C D9 86 F1 C0 92 89 FB 97 E6 FB D0 EA 56 EB 59 EF CF 18 AF 97 5D DE FD A4 67 B0 87 89 05 2E 2E
0000033C  A8 6D F6 BD FB 99 F4 F1 5F 00 42 9A 85 D8 BD E0 EE 67 CA EF 0F 31 77 64 36 C4 6E 63 9F 0A 18 01 F7 26 90 7C
00000360  27 F7 76 6E B8 45 22 9D A9 26 F0 A3 86 83 AA 60 D2 DA B8 D4 80 64 D0 BC 5D C8 C3 0A 67 BB 57 14 E6 29 4C ED
00000384  F3 B8 6B F9 2E 08 CB B8 02 5B AC 6D 25 DB 9D CD F9 9C 05 83 6D 56 7A C4 C1 67 21 02 B6 16 05 B1 6F 45 9C 9B
000003A8  6F 9C 65 4E 80 C5 E2 08 0A E3 6F 35 38 1D 8A 34 65 09 B6 FA 39 D2 21 0C CE 97 08 C1 A8 28 21 BA 47 02 C1 4F
000003CC  A2 7E 2C 6B 81 A1 56 9B 1C 4B 17 AF F8 A1 24 09 5D D6 6E 15 C8 55 13 4C D4 44 0A F4 D9 4F 51 C2 65 64 9A AA
000003F0  F6 37 9C 28 59 64 CA CA 10 7A 49 F9 87 C0 65 7A EA CD 9D A1 51 AF 06 B5 88 B0 E2 45 7B D9 DC D0 82 63 5E C9
00000414  D2 2A 23 A8 7B A8 00 BF F9 01 2B D0 4E 99 29 64 6B 35 08 01 1E 17 AC AF AE 07 CE 8F 71 7A 0A E4 13 DE FB 52
00000438  50 6E B7 FB 87 F8 A6 AF 82 26 0E 3F C1 DE 8E 30 EF 1F 15 32 E5 99 02 E6 57 44 48 D9 A0 07 E5 71 94 7B 0F F6
0000045C  51 A4 A1 00 67 A8 0E 64 74 A1 EE 17 48 94 87 7A 96 B4 D6 77 90 2F 84 05 E3 D7 D9 88 70 64 DC 02 CB 84 13 3A
00000480  BC FE AF AC 4A 36 46 DC 00 0D AA 77 25 9E C4 52 00 F8 64 83 E9 CC 4E 3C 5F AF 9C A1 AF 75 B6 9E BF 60 A8 0E
000004A4  F9 F4 D9 F6 FB 05 CC BF 3B F0 C2 DB 66 C6 E8 03 C6 2F D9 1C 1E 45 17 76 C0 E4 89 42 B3 2B 08 4E A5 89 B1 68
000004C8  54 FF 28 59 ED CA 82 E3 FA CA C4 78 56 C5 FB 00 33 D4 B0 6A 73 35 FF D9 EF 46 F0 65 87 8E 2D 45 4A E2 50 FB
000004EC  08 E8 2F 8D 56 9B 3F 34 8A 3A 92 1D C3 6F 7B A9 10 D1 00 5D 58 15 ED 1C 96 4A B2 76 F6 D0 1F 20 55 79 4D 3A
00000510  DF 7D 23 6F 52 82 5E 97 F0 A0 38 4A 30 54 E2 26 C4 19 D7 76 BB 8B 7E 89 2B 99 C1 D6 F3 9B D6 B1 1A 8F 18 A4
```

v. k1=12 34 56 78 9A BC DE F0 ,,, k2=12 23 34 56 78 9A BC ED

first time using k1



CrypTool 1.4.42 - DES (ECB) encryption of <8_1 text>, key <12 34 56 78 9A BC DE F0>

File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help

8_1 text

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

1) The starting page of th
The starting page of the
Press F1 to start the onli

2) A possible next step w

3) There are several exar

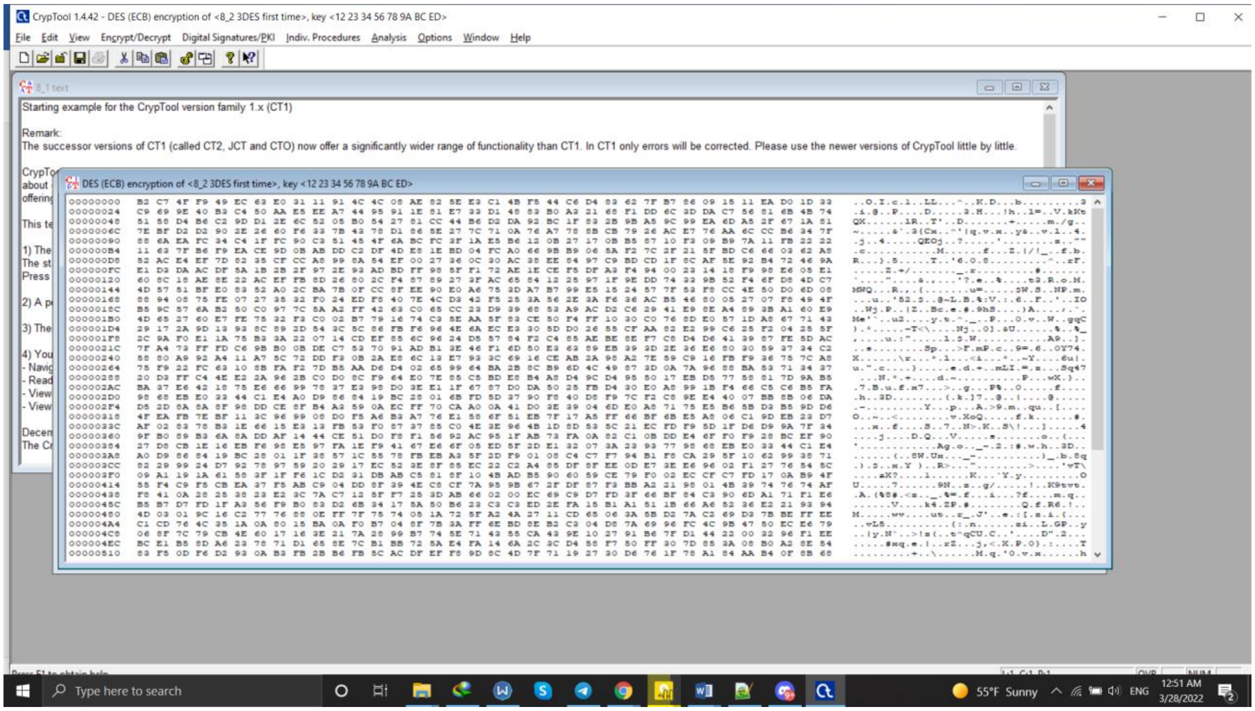
4) You can further develo
- Navigating playfully thro
- Reading the included re
- Viewing the included co
- Viewing the webpage w

December 2021
The CrypTool Team

DES (ECB) encryption of <8_1 text>, key <12 34 56 78 9A BC DE F0>

```
00000000  E0 3B 63 14 A3 0F C8 37 E0 1D 94 98 39 38 C1 63 2F 4C 62 7A 4F 12 18 DA D4 96 A0 B0 A2 5E 27 92 9C 0E 19 50
00000024  96 53 44 27 4D 07 6F B2 2F 46 1F 16 DA C7 EA 42 30 3E 78 B5 02 E5 2E C2 57 D6 98 E9 1C 6C 20 98 2B DC DB 5A
00000048  E5 2A 93 9E 3B E6 69 78 F0 CD AB C7 C2 79 A6 2D B6 1C 48 E6 09 49 06 A5 24 5A 26 39 CC 84 13 64 5C F9 7D 89
0000006C  7B 13 83 6C 64 CF C0 C2 8E E2 19 DE A7 0A 4D 8A 05 BA 31 AA 7C 63 CF C2 A0 97 F0 9D 80 91 46 5D 1F F2 88 BA
00000090  0E 8C C1 12 81 F3 2C 19 B1 0B B8 33 D9 2D DF FA DB 54 39 C8 D3 FB 9F 96 A1 B0 42 9E C5 0F EC BC 13 FD 8F AE
000000B4  A2 82 05 21 6D 99 02 99 95 38 51 16 74 A5 D9 C1 0B 21 36 75 69 4F 24 38 FA AE 8D 10 27 7C E9 AC C5 86 97 74
000000D8  89 BA C5 F8 4D A4 4E B1 AA 03 EE 31 EA FC B2 AB 4F 66 55 17 26 F1 DD E0 27 4F 65 F0 85 37 34 37 5C 67 58 9A
000000FC  69 9D 9D DE 19 B7 A4 58 B4 2B 48 E3 3F D7 C1 DB 09 AD B2 4E C9 6C 1D 20 23 84 C3 37 B8 81 88 65 D6 59 BF 77
00000120  AC DE 99 15 F9 49 DC 63 A6 CA EB 65 29 CB 15 17 BB 58 17 0E 4C E2 52 96 80 52 36 07 C0 24 96 DE 29 9E A5 E8
00000144  71 11 F1 A0 60 2C 9D D8 68 F0 52 86 AA EC 03 AA 41 94 13 2E 89 16 F5 9D 74 0F 43 3C A3 2C 1C D2 36 93 8E 75
00000168  9C 10 94 A8 F4 BD 77 CB 3D A1 E0 75 B9 25 B5 CB A5 C6 1B 6F DE 7A 8E 68 BF 7E F9 E3 38 A4 E3 26 83 07 A2 38
0000018C  B8 76 D1 62 5E 6D 7E 12 60 3B FE 10 3A B3 D7 54 34 D2 B8 79 B5 74 26 D5 F6 CE 61 67 29 07 CA B9 D7 8C AC BD
000001B0  F8 38 4D 1B 48 35 D0 A0 42 28 7B EC C9 C7 CA 7E 81 F9 37 F8 60 7F E2 3A 3E AD 1E C5 0D 92 24 B9 02 CD A5 89
000001D4  D6 8A DA 94 A2 CE 36 44 18 CE FE 72 D2 CE 57 D6 BF 51 CD C8 64 B4 6F 55 76 CC 49 99 58 6E EC DE FF 44 FD 38
000001F8  FB F1 99 4D 0F F4 A7 FE 0E 64 53 F8 34 01 B7 7C 8F 6E 3A 89 1C CF 62 D9 97 34 42 3B CD 67 0A 3F 41 31 62 75
0000021C  02 7C D2 85 48 1C A5 E8 D8 D3 80 7D 3C E4 41 50 38 0E 0D E3 42 9A 6E 65 03 80 89 04 97 87 86 DF 1E A6 BC 14
00000240  75 2C BE 5D 1C F7 1D 83 19 63 D6 5C FA 38 91 27 D3 C6 98 8D 11 88 49 D4 FB 6E 54 F6 79 96 01 B0 6E 64 44 57
00000264  2A A1 90 08 00 EC 9E 06 C9 9A 2C 6C B6 1E 59 2D 8A 9F 9D E8 26 0E 2D E4 76 92 22 4A BD B4 92 66 D6 75 0B C5
00000288  5C BF 66 92 D8 83 23 B6 BA DD 0C 52 27 1E 33 2C FE 8C 93 D2 12 07 2F 69 90 FD EC 22 40 03 05 67 7E 84 43 7D
000002AC  D0 88 6A FE 74 72 52 F5 47 5B 5F 37 67 05 FE 28 7C 1F 2D 97 6A 00 E4 0A 67 DA 79 F9 CD FA 9C 5A 97 7C DB FC
000002D0  19 59 84 4B 18 7E 4D EA E0 BF 91 F0 DD 20 B8 89 06 60 C2 0E 1E 19 46 85 1D F9 58 8F 67 A1 5C B2 DD 27 F9 D1
000002F4  CE 00 D8 80 DA 2C D0 60 95 D2 5F DD B7 18 4B 6B 99 1D 27 71 87 9D A7 58 9A C7 2A 84 6A 80 8E 7E D2 B9 19 B8
00000318  3C 79 79 7A 9E 51 A5 06 A0 9B 4E CF 2A E4 23 28 F2 30 37 1A 00 1A 96 05 D0 5C F2 75 C0 FF 18 21 70 65 1E 10
0000033C  44 69 2A F7 41 64 18 35 65 59 83 A9 1E DA 0E 57 B4 F2 5A D6 3C 1B BE E9 E2 63 F6 86 FC CE 72 39 25 08 15 6C
00000360  14 E6 B0 BD 21 6B C0 62 D7 AB 4D 1D 2D 9D E0 8E 1C 72 6C 31 46 C0 1E 54 A5 96 01 CA F7 D8 BE 92 C9 8E BB B5
00000384  25 D1 D1 36 8D 96 6B 59 5A 40 39 2B BF F1 3B 01 3E 1F 05 98 EF 16 CD 4D DD 63 8B 28 19 59 84 4B 18 7E 4D EA
000003A8  E0 BF 91 F0 DD 20 B8 89 4D 4F 75 A0 5F 0B 60 BF D2 87 EB EB 10 C3 45 5B EF FB C0 F1 2D 90 07 4F E9 BD CE B1
000003CC  91 23 49 2C B8 C9 BD B6 F9 95 D6 7B 77 95 99 5E 7B FD 71 9A 8E 33 2C 42 4D 29 1D C2 99 D8 46 DA 2A A5 EA 7D
000003F0  C8 C4 28 2C C5 F9 7C D8 B3 96 A6 0A 78 67 E6 EE EE 86 6D DF BF A7 38 6F CA 99 BD DD AE 4E F1 90 D9 85 9D E6
00000414  F3 5C D7 DA E8 DB BB 2C E8 3B DB E5 D5 0D 13 37 E0 6C 45 B2 5F 6C 47 13 8E 33 C5 2D 1D 80 14 10 11 70 F9 74
00000438  FD 22 09 CF CC D5 84 1C 51 E5 7F 5C 83 07 B9 E1 46 07 7F 87 69 9B 4A B5 90 45 FD C8 07 6F B7 31 65 D5 79 E6
0000045C  C4 22 36 06 AB F7 50 D8 18 DB 66 F2 27 10 F6 87 BB F1 0A 4B ED 4E E7 BF 93 4A 4E C2 46 CF A0 B8 21 1B AC E2
00000480  A3 39 EB 37 B6 82 46 4D 6B 06 DE 04 18 55 F3 E8 E6 BB 82 52 12 88 6A 95 37 C5 B1 03 C8 FE C7 1A F4 CA 32 61
000004A4  7A 69 88 94 0B 1A 67 E5 A0 40 0B 9E FB D3 1D F6 64 40 D1 42 C8 25 E8 90 8C 9E 00 0D 2F 81 84 37 DB 80 FA D6
000004C8  CC C4 5C EE 85 B4 EB 48 64 59 E8 56 FD 5D 06 CC 3C 6F E5 48 D2 36 1E E9 7E A3 5D 31 21 5F FD 6E 56 32 8B 5B
000004EC  46 C1 51 A1 E5 28 05 81 AC 14 FE 44 18 BC 28 B7 47 5F 3E AC 43 DB 69 FA 01 07 49 4C 6C 07 71 48 C2 2B 9A C4
00000510  E0 27 2F 9A 38 E5 35 8A 3A E5 15 5E F4 8F 42 82 4A B0 01 D4 4D 55 B7 97 9D AD 99 14 E9 6A 58 FE 94 27 AE B6
```

second time using k2


CrypTool 1.4.42 - DES (ECB) encryption of <8_2 3DES first time>, key <12 23 34 56 78 9A BC ED>
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
8_1 text
Type here to search
55°F Sunny
ENG
12:51 AM
3/28/2022

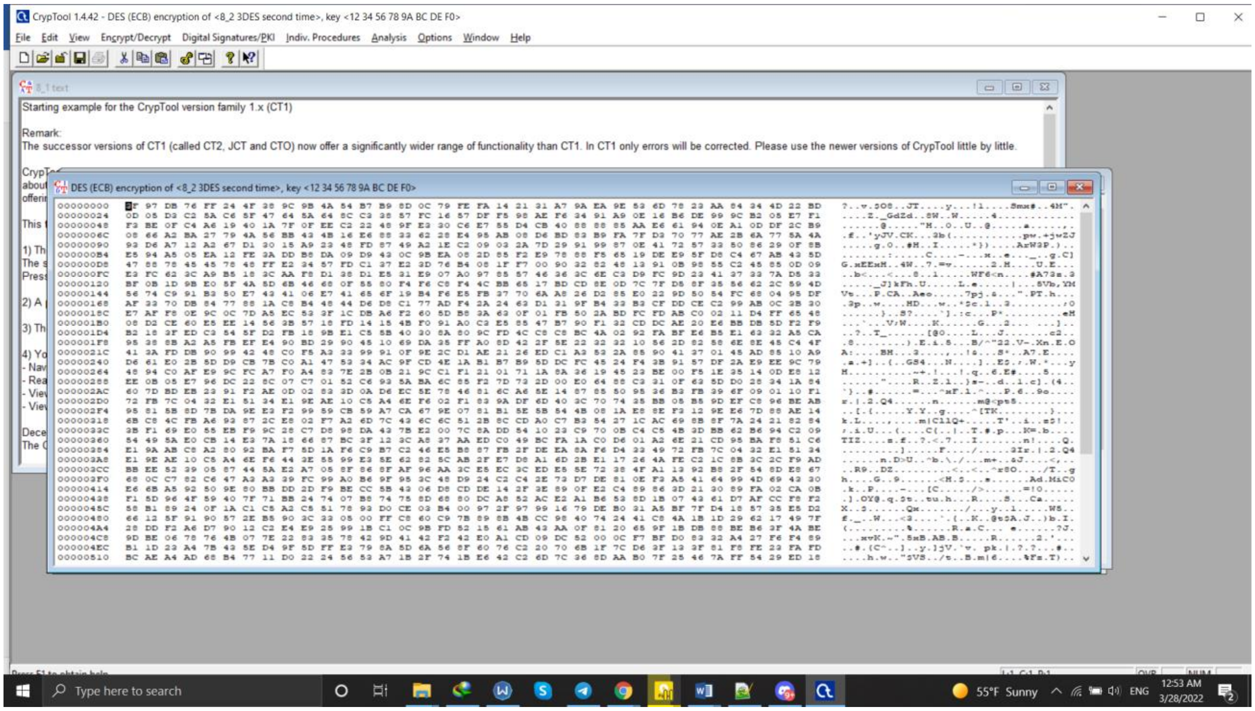
Starting example for the CrypTool version family 1.x (CT1)

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.

DES (ECB) encryption of <8_2 3DES first time>, key <12 23 34 56 78 9A BC ED>

```
00000000  B2 C7 4F F9 49 EC 63 E0 31 11 91 4C 4C 08 AE 82 5E E3 C1 4B F5 44 C6 D4 83 62 7F B7 86 09 18 11 EA D0 1D 33
00000024  C9 69 9E 40 B3 C4 50 AA E5 EE A7 44 95 91 1E 81 E7 33 D1 48 83 B0 A3 21 68 F1 DD 6C 3D DA C7 56 81 6B 4B 74
00000048  51 58 D4 B6 C2 9D D1 2E 6C 52 05 B0 54 27 81 CC 44 B6 D2 DA 92 BC 1F 83 2B 9B A5 9C 99 EA 6D A5 2F 67 1A 81
0000006C  7E BF D2 D2 90 2E 26 60 F6 33 7B 43 78 D1 86 5E 27 7C 71 0A 76 A7 78 8B CB 79 26 AC E7 76 AA 6C CC B6 34 7F
00000090  88 6A EA FC 34 C4 1F FC 90 C3 81 45 4F 6A BC FC 3F 1A E5 B6 12 0B 27 17 0B B5 87 10 F3 09 B9 7A 11 FB 22 22
000000B4  11 63 7F B6 F9 EA CE 9D 0B AB DD C2 DF 4D E8 1E BD 04 FC A0 66 9B B9 06 5A F2 7C 2F 21 8F BD C6 66 03 62 A8
000000D8  52 AC E4 EF 7D 82 35 CF CC A8 99 8A 54 EF 00 27 36 0C 30 AC 38 EE 84 97 C9 BD CD 1F 8C AF 5E 92 B4 72 46 9A
000000FC  E1 D3 DA AC DF 5A 1B 2B 2F 97 2E 93 AD BD FF 98 5F F1 72 AE 1E CE F5 DF A3 F4 94 00 23 14 18 F9 98 E6 05 E1
00000120  60 8C 18 AE 8E 22 AC EF FB 8D 26 80 2C F4 87 89 27 3F AC 65 84 12 25 97 1F 9E DD 74 33 9B 52 F4 6F D8 4D C7
00000144  4D 57 51 BF E0 83 52 A0 2C BA 7B 0F CC 8F EE 90 E0 A6 75 3D A7 B7 99 E5 15 24 57 7F 53 F8 CC 4E 50 D0 6D 08
00000168  88 94 08 75 FE 07 27 35 32 F0 24 ED F8 40 7E 4C D3 42 F5 25 3A 56 2E 3A F6 36 AC B5 46 80 05 27 07 F8 49 4F
0000018C  B5 9C 57 6A B2 50 C0 97 7C 5A A2 FF 42 63 C0 65 CC 23 D9 39 68 53 A9 AC D2 C6 29 41 E9 8E A4 89 3B A1 60 E9
000001B0  4D 65 27 60 E7 FE 78 32 F3 C0 02 B7 79 16 74 C3 5E AA 5F 83 CE 50 F4 FF 10 30 C0 76 8D E0 57 1D A8 67 71 43
000001D4  29 17 2A 9D 13 93 8C 89 2D 54 3C 5C 86 FB F6 96 4E 6A EC E3 30 5D D0 26 55 CF AA 82 E2 99 C6 25 F2 04 25 5F
000001F8  2C 9A F0 E1 1A 75 B3 3A 22 07 14 CD EF 85 6C 96 24 D5 57 84 F2 C4 85 AE BE 8E F7 C8 D4 D6 41 39 87 FE 5D AC
0000021C  7F A4 73 FF FD C6 9B B0 0B DE C7 53 70 91 AD B1 3E 46 F1 6D 50 E3 63 89 EB 39 3D 2E 36 E6 80 30 59 37 34 C2
00000240  58 80 A9 92 A4 11 A7 5C 72 DD F3 0B 2A E8 6C 13 E7 93 3C 69 16 CE AB 2A 98 A2 7E 59 C9 16 FB F9 36 75 7C A8
00000264  75 F9 22 FC 63 10 8B FA F2 7D B5 AA D6 D4 02 65 99 64 BA 2B 8C B9 6D 4C 49 87 3D 0A 7A 96 88 BA 53 71 34 37
00000288  20 D3 FF C4 4E E2 2A 96 2B C0 D0 8C F9 64 E0 7E 85 C5 BD E8 B4 A8 D4 9C D4 95 80 17 EB D5 77 58 81 7D 9A B5
000002AC  BA 37 E6 42 18 75 E6 66 99 78 37 E3 98 D0 3E E1 1F 67 87 D0 DA 50 25 FB D4 30 E0 A8 99 1B F4 66 C5 C6 B5 FA
000002D0  98 68 EB E0 33 44 C1 E4 A0 D9 86 84 19 BC 28 01 6B FD 5D 37 90 F8 40 D8 F9 7C F2 C8 9E E4 40 07 BB 8B 06 DA
000002F4  D5 2D 8A 8A 8F 98 DD CE 8F B4 A3 59 0A EC FF 70 CA A0 0A 41 D0 3E 39 04 6D E0 A8 71 75 E5 B6 5B D3 B5 9D D6
00000318  4F EA FB 7E BF 11 3C 96 99 08 D0 F5 A6 B3 A7 76 E1 58 6F 51 EB 7F 17 A5 FF 66 BF 6B E5 A8 06 C1 9D EB 23 D7
0000033C  AF 02 83 78 B3 1E 66 15 E3 13 FB 53 F0 87 37 85 C0 4E 3E 96 4B 1D 8D 53 5C 21 EC FD F9 5D 1F D6 D9 9A 7F 34
00000360  9F B0 89 B3 6A 8A DD AF 14 44 CE 81 D0 F8 F1 56 92 AC 95 1F AB 73 FA 0A 82 C1 0B DD E4 6F F0 F9 28 BC EF 90
00000384  27 D8 CB 1E 16 EB F6 98 E5 97 FA 1E F9 41 67 E6 6F 05 ED 5F 2D E1 32 07 3A 23 93 77 98 68 EB E0 33 44 C1 E4
000003A8  A0 D9 86 84 19 BC 28 01 1F 38 57 1C 88 78 FB EB A3 5F 2D F9 01 08 C4 C7 F7 94 B1 F8 CA 29 5F 10 62 99 38 71
000003CC  82 29 99 24 D7 92 78 97 59 20 29 17 EC 52 3E 8F 85 EC 22 C2 A4 85 DF 8F EE 0D E7 3E E6 96 02 F1 27 76 54 5C
000003F0  09 A1 19 1A 61 58 3F 1F F6 1C D2 31 DB AB C5 81 8F 10 4B AD B5 90 60 59 CE 79 F0 02 EC CF C7 FD 17 0A B9 4F
00000414  55 F4 C9 F5 CB EA 37 F5 AB C9 04 DD 8F 39 4E C8 CF 7A 95 9B 67 2F DF 87 F3 BB A2 21 98 01 4B 39 74 76 74 AF
00000438  F8 41 0A 28 25 38 23 E2 3C 7A C7 12 8F F7 25 3D AB 66 02 00 EC 69 C9 D7 FD 3F 66 BF 84 C3 90 6D A1 71 F1 E6
0000045C  B5 B7 D7 FD 1F A3 56 F9 B0 83 D2 6B 34 17 5A 50 B6 23 C3 C3 ED 2E FA 18 B1 A1 51 1B 66 A6 52 36 E2 21 93 94
00000480  4D 03 01 9C 16 C2 77 76 88 0E FF 7F 75 74 05 1A 72 5F A2 4A 27 11 CD 65 06 3A 5B D2 7A C2 69 D3 7B BE FF EE
000004A4  C1 CD 76 4C 35 1A 0A 80 15 BA 0A F0 B7 04 8F 7B 3A FF 6E BD 8E B2 C3 04 D8 7A 69 96 FC 4C 9B 47 50 EC E6 79
000004C8  06 8F 7C 79 CB 4E 60 17 16 3E 21 7A 28 99 B7 74 5E 71 43 55 CA 43 9E 10 27 91 B6 7F D1 44 22 00 32 96 F1 EE
000004EC  BC E1 B5 8D A6 23 78 71 D1 65 8E 7C B1 BB 72 5A E4 FA 14 6A 2C 3C D4 58 F7 50 FF 30 7D 85 3A 08 B0 A2 8E 54
00000510  83 F5 0D F6 D2 93 0A B3 FB 2B B6 FB 5C AC DF EF F8 9D 8C 4D 7F 71 19 27 30 D6 76 1F 78 A1 84 AA B4 0F 8B 68
```

third time using k1


CrypTool 1.4.42 - DES (ECB) encryption of <8_2 3DES second time>, key <12 34 56 78 9A BC DE F0>
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
8_1 text
Type here to search
55°F Sunny
ENG
12:53 AM
3/28/2022

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

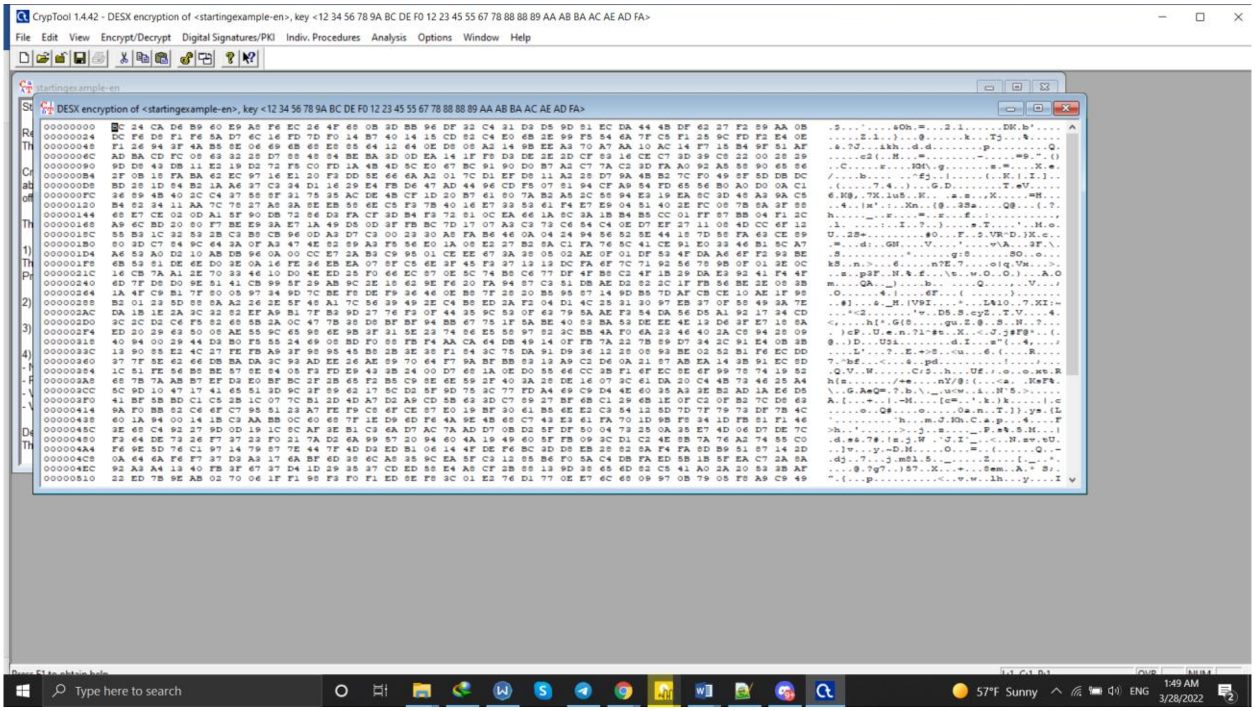
Remark:
The successor versions of CT1 (called CT2, JCT and CTO) now offer a significantly wider range of functionality than CT1. In CT1 only errors will be corrected. Please use the newer versions of CrypTool little by little.

DES (ECB) encryption of <8_2 3DES second time>, key <12 34 56 78 9A BC DE F0>

```
00000000  3F 97 DB 76 FF 24 4F 38 9C 9B 4A 84 B7 B9 8D 0C 79 FE FA 14 21 31 A7 9A EA 9E 53 6D 78 23 AA 84 34 4D 22 BD
00000024  0D 05 D3 C2 5A C6 8F 47 64 5A 64 8C C3 38 57 FC 16 57 DF F5 98 AE F6 34 91 A9 0E 16 B6 DE 99 9C B2 05 E7 F1
00000048  F3 BE 0F C4 A6 19 40 1A 7F 0F EE C2 22 48 9F E3 30 C6 E7 55 D4 CB 40 88 88 85 AA E6 61 94 0E A1 0D DF 2C B9
0000006C  08 66 A2 BA 27 79 4A 56 BB 43 4B 16 E6 88 33 62 28 E4 95 AB 08 D6 BD 83 B9 FA 7F D3 70 77 AE 2B 6A 77 5A 4A
00000090  93 D6 A7 12 A2 67 D1 30 15 A9 23 48 FD 87 49 A2 1E C2 09 03 2A 7D 29 91 99 87 0E 41 72 57 33 50 86 29 0F 8B
000000B4  E5 94 A5 05 EA 12 FE 3A DD B8 DA 09 D9 43 0C 9B EA 08 2D 85 F2 E9 78 88 F5 65 19 DE E9 5F D8 C4 67 AB 43 5D
000000D8  47 88 78 45 45 78 48 FF E2 34 57 FD C1 37 E2 3D 76 B4 08 1F F7 00 90 32 82 48 13 91 0B 98 55 C2 45 85 0D 09
000000FC  E3 FC 62 3C A9 B5 18 3C AA F8 D1 38 D1 E5 31 E9 07 A0 97 85 57 46 36 3C 6E C3 D9 FC 9D 23 41 37 33 7A D5 33
00000120  BF 0B 1D 9B E0 5F 4A 5D 6B 46 68 0F 55 80 F4 F6 C8 F4 4C BB 65 17 BD CD 8E 0D 7C 7F D5 8F 35 56 62 2C 59 4D
00000144  56 74 C9 91 B3 50 E7 43 41 06 E7 41 65 6F 19 B4 F6 E5 FB 37 70 6A A8 26 D2 85 E0 22 9D 50 54 FC 68 04 95 DF
00000168  AF 33 70 DB 84 77 88 1A C8 B4 48 44 D6 D8 C1 77 AD F4 2A 24 63 D1 31 9F B4 33 B3 CF DD CE C2 99 AB 0C 3B 30
0000018C  E7 AF F8 0E 9C 0C 7D A5 EC 53 3F 1C DB A6 F2 60 5D B8 3A 63 0F 01 FB 50 2A BD FC FD AB C0 02 11 D4 FF 65 48
000001B0  08 D2 CE 60 E5 EE 14 56 3B 57 18 FD 14 15 4B F0 91 A0 C3 E5 85 47 B7 90 F1 32 CD DC AE 20 E6 BB DB 5D F2 F9
000001D4  B2 18 3F ED C3 54 5F D2 FB 18 9B E1 C5 5B 40 30 8A 80 9C FD 4C C8 C8 BC 4A 02 92 FA BF E6 B5 E1 63 32 A5 CA
000001F8  95 38 8B A2 A5 FB EF E4 90 BD 29 90 45 10 69 DA 35 FF A0 8D 42 2F 8E 22 32 32 10 56 2D 82 58 6E 8E 45 C4 4F
0000021C  41 3A FD DB 90 99 42 48 C0 F5 A3 33 99 91 0F 9E 2C D1 AE 21 26 ED C1 A3 53 2A 85 90 41 37 01 45 AD 85 10 A9
00000240  D6 61 E0 2B 8D D9 CB 7B C0 A1 47 53 34 AC 9F CD 4E 1A B1 B7 B9 5D DC FC 45 24 F4 3B 91 57 DF 2A E9 EE 9C 79
00000264  48 94 C0 AF E9 9C FC A7 F0 A4 83 7E 2B 0B 21 9C C1 F1 21 01 71 1A 8A 36 19 45 23 BE 00 F5 1E 35 14 0D E8 12
00000288  EE 0B 05 E7 96 DC 22 8C 07 C7 01 52 C6 93 5A BA 6C 85 F2 7D 73 2D 00 E0 64 88 C3 31 0F 63 5D D0 28 34 1A 84
000002AC  60 7D BD EB 23 91 F2 AE 0D 02 83 3D 0A D6 EC 5E 78 46 81 6C A6 8E 14 87 85 50 95 36 B3 FB 39 6F 09 01 10 F1
000002D0  72 FB 7C 04 32 E1 51 34 E1 9E AE 10 C5 A4 6E F6 02 F1 83 9A DF 6D 40 3C 70 74 35 BB 05 B5 9D EF C8 96 BE AB
000002F4  95 81 5B 8D 7B DA 9E E3 F2 99 59 CB 59 A7 CA 67 9E 07 81 B1 5E 5B 54 4B 08 1A E8 8E F3 12 9E E6 7D 88 AE 14
00000318  6B C8 4C FB A6 93 87 2C E8 02 F7 A2 6D 7C 43 6C 6C 51 2B 8C CD A0 C7 B3 54 27 1C AC 69 8B 8F 7A 24 21 82 84
0000033C  3B F1 69 E0 55 EB F9 9C 28 C7 D8 98 DA 43 7B E2 00 7C 8A DD 54 10 23 C9 70 0B C4 C5 4B 3D BB 62 B6 94 C2 09
00000360  54 49 5A E0 CB 14 E3 7A 18 66 87 BC 3F 12 3C A8 37 AA ED C0 49 BC FA 1A C0 D6 01 A2 6E 21 CD 98 BA F8 51 C6
00000384  E1 9A AB C8 A2 80 92 BA F7 5D 1A F6 C9 B7 C2 46 E5 B8 87 FB 2F DE EA 8A F6 D4 33 49 72 FB 7C 04 32 E1 51 34
000003A8  E1 9E AE 10 C5 A4 6E F6 44 3E 55 99 E3 5E 62 82 5C AB 2F E7 D8 A1 6D 2B E1 17 26 4A FE C2 1C 8B 3C 2C F9 AD
000003CC  BB EE 52 39 05 87 44 5A E2 A7 05 8F 86 8F AF 96 AA 3C E5 EC 3C ED E5 5E 72 38 4F A1 13 92 B8 2F 54 8D E8 67
000003F0  68 0C C7 82 C6 47 A3 A3 39 FC 99 A0 B6 9F 95 3C 48 D9 24 C2 C4 2E 73 D7 DE 81 0E F3 A5 41 64 99 4D 69 43 30
00000414  E6 6B A5 92 50 9E 80 BB DD 2D F9 BE CC 5B 43 06 D8 CD DE 14 2F 3E 89 0F E2 C4 89 86 3D 21 30 89 FA 02 CA 0B
00000438  F1 5D 96 4F 59 40 7F 71 BB 24 74 07 B8 74 75 8D 68 80 DC A8 52 AC E2 A1 B6 53 8D 1B 07 43 61 D7 AF CC F8 F2
0000045C  58 B1 89 24 0F 1A C1 C5 A2 C5 51 78 93 D0 CE 03 B4 00 97 2F 97 99 16 79 DE B0 31 A5 BF 7F D4 18 57 35 E5 D2
00000480  66 12 5F 91 90 57 2E B5 90 3C 33 05 00 FF C8 60 C9 7B 89 8B 4B CC 98 40 74 24 41 C8 4A 1B 1D 29 62 17 49 7F
000004A4  28 DD F2 A6 D7 90 12 C2 E4 E9 25 99 1B C1 0C 9B FD 52 15 61 AB 43 AA 0F 81 20 65 9F 1B DB 88 BE B6 3F 4A BE
000004C8  9D BE 06 78 76 4B 07 7E 22 83 35 78 42 9D 41 42 F2 42 E0 A1 CD 09 DC 52 00 0C F7 BF D0 83 32 A4 27 F6 F4 89
000004EC  B1 1D 23 A4 7B 43 5E D4 9F 5D FF E3 79 8A 5D 6A 56 8F 60 76 C2 20 70 6B 1F 7C D6 3F 13 3F 81 F8 FE 23 FA FD
00000510  BC AE A4 AD 68 B4 77 11 D0 22 24 56 53 A7 1B 2F 74 1B E6 42 C2 6D 7C 36 8D AA B0 7F 25 46 7A FF 54 29 ED 18
```

## 8.3 :

i. key 12 34 56 78 9A BC DE F0 12 23 45 55 67 78 88 88 89 AA AB BA AC AE AD FA

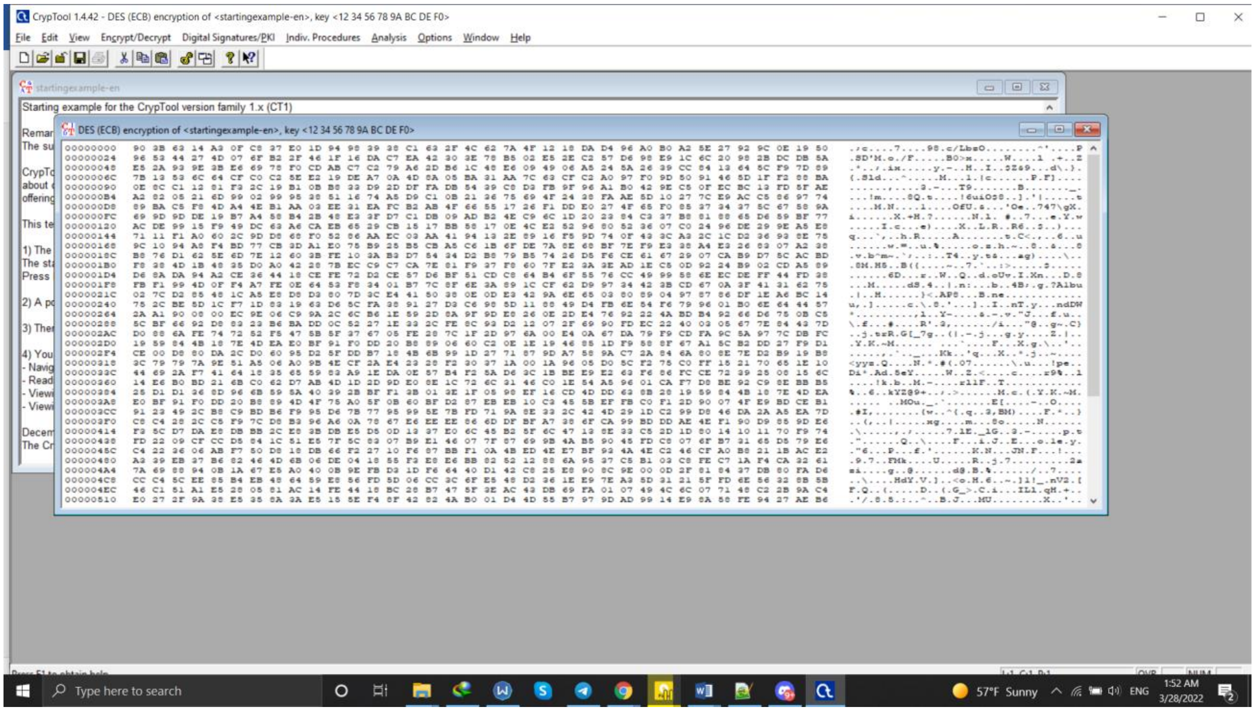


CrypTool 1.4.42 - DESX encryption of <startingexample-en>, key <12 34 56 78 9A BC DE F0 12 23 45 55 67 78 88 88 89 AA AB BA AC AE AD FA>

DESX encryption of <startingexample-en>, key <12 34 56 78 9A BC DE F0 12 23 45 55 67 78 88 88 89 AA AB BA AC AE AD FA>

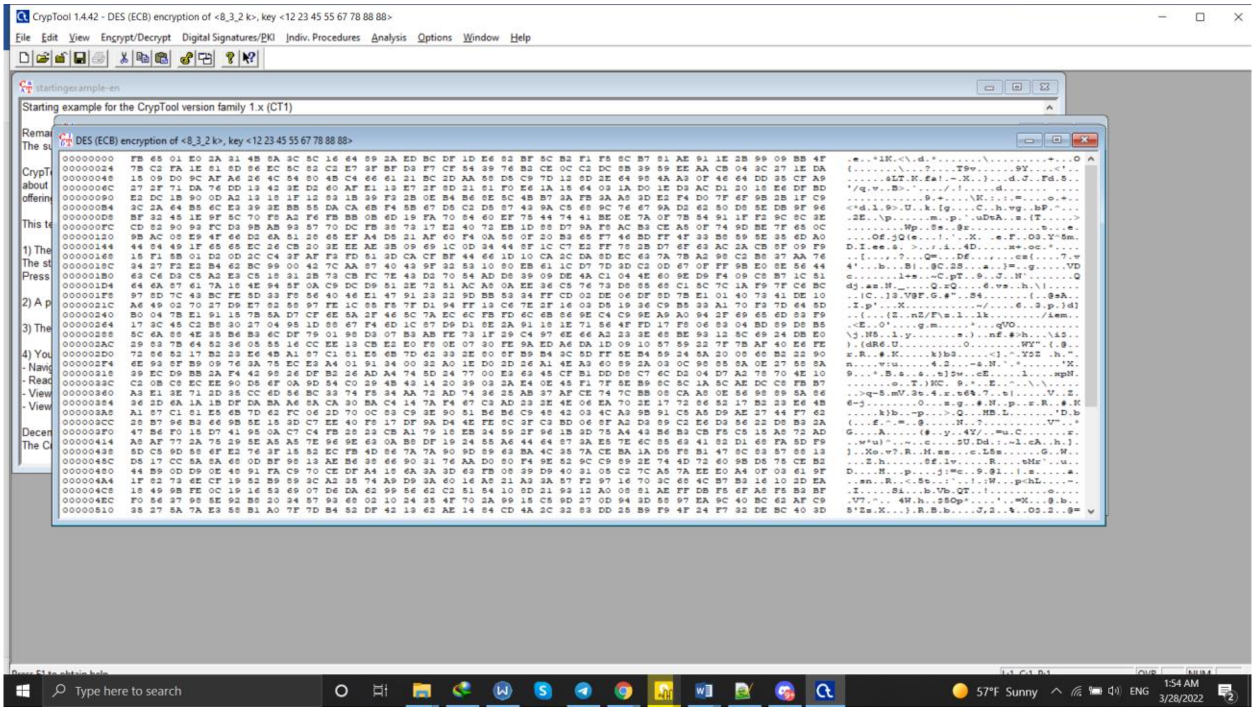
```
00000000   8C 24 CA D6 B9 60 E9 A8 F6 EC 26 4F 68 0B 3D BB 96 DF 32 C4 31 D3 D5 9D 81 EC DA 44 4B DF 62 27 F2 89 AA 0B   .$...`....&Oh.=...2.1......DK.b'....
00000024   DC F6 D8 F1 F6 5A D7 6C 16 FD 7D F0 14 B7 40 14 15 CD 82 C4 E0 6B 2E 99 F5 54 6A 7F C5 F1 25 9C FD F2 E4 0E   .....Z.l..}...@......k...Tj...%.....
00000048   F1 26 94 3F 4A B5 8E 06 69 6B 68 E8 85 64 12 64 0E D8 08 A2 14 9B EE A3 70 A7 AA 10 AC 14 F7 15 B4 9F 51 AF   .&.?J...ikh..d.d........p.........Q.
0000006C   AD BA CD FC 08 63 32 28 D7 88 48 84 BE BA 3D 0D EA 14 1F F8 D3 DE 2E 2D CF 83 16 CE C7 3D 39 C8 22 00 28 29   .....c2(..H...=........-.....=9.".()
00000090   9D D8 43 DB 11 E2 19 D2 72 F5 C0 FD 1A 4B 4D 5C E0 67 BC 91 90 D0 B7 A2 C7 7A C2 3D FA A0 92 A5 58 90 65 86   ..C.....r....KM\.g.......z.=....X.e.
000000B4   2F 0B 18 FA BA 62 EC 97 16 E1 20 F3 DD 5E 66 6A A2 01 7C D1 EF D8 11 A2 28 D7 9A 4B B2 7C F0 49 8F 5D DB DC   /....b.... ..^fj..|.....(..K.|.I.]..
000000D8   BD 28 1D 84 B2 1A A6 37 C3 34 D1 16 29 E4 FB D6 47 AD 44 96 CD F5 07 81 94 CF A9 54 FD 65 56 B0 A0 D0 0A C1   .(.....7.4..)...G.D.......T.eV......
000000FC   36 89 4B 40 2C C4 37 58 8F 31 75 35 AC DE 4B CF 1D 20 B7 61 80 7A B2 A5 2C 58 94 E3 19 EA 8C 3D 48 A3 9A C5   6.K@,.7X.1u5..K.. .a.z..,X.....=H...
00000120   B4 82 34 11 AA 7C 78 27 A8 3A 8E EB 58 6E C5 F3 7B 40 16 E7 33 53 61 F4 E7 E9 04 51 40 2E FC 08 7B 8A 3F 88   ..4..|x'.:..Xn..{@..3Sa....Q@...{.?.
00000144   68 E7 CE 02 0D A1 5F 90 DB 72 86 D3 FA CF 3D B4 F3 72 81 0C EA 66 1A 8C 3A 1B B4 B5 CC 01 FF 87 BB 04 F1 2C   h....._..r....=..r...f..:..........,
00000168   A9 6C BD 20 80 F7 BE E9 3A E7 1A 49 D5 0D 3F FB BC 7D 17 07 A3 C3 73 C6 84 C4 0E D7 EF 27 11 08 4D CC 6F 12   .l. ....:..I..?..}.....s.......'..M.o.
0000018C   55 B3 1C 32 53 2B C3 B8 CB 96 0D A3 D7 C3 00 23 30 A8 FA B6 46 0A 04 24 94 56 52 5E 44 18 7D 58 FA 63 CE 89   U..2S+.........#0...F..$.VR^D.}X.c..
000001B0   80 3D C7 84 9C 64 3A 0F A3 47 4E 82 89 A3 F5 56 E0 1A 08 E2 27 B2 8A C1 FA 76 5C 41 CE 91 E0 33 46 B1 5C A7   .=...d:..GN....V....'....v\A...3F.\.
000001D4   A6 53 A0 D2 10 AB DB 96 0A 00 CC E7 2A B3 C9 95 01 CE EE 67 3A 38 05 02 AE 0F 01 DF 53 4F DA A6 6F F2 93 BE   .S..........*......g:8......SO..o...
000001F8   6B 53 81 DE 6E D0 3E 0A 16 FE 36 EB EA 07 8F C5 6E 3F 45 F3 37 13 13 DC FA 6F 7C 71 92 56 78 9B 0F 01 3E 0C   kS..n.>...6.....n?E.7.....o|q.Vx...>.
0000021C   16 CB 7A A1 2E 70 33 46 10 D0 4E ED 25 F0 66 EC 87 0E 5C 74 B8 C6 77 DF 4F B8 C2 4F 1B 29 DA E3 92 41 F4 4F   ..z..p3F..N.%.f...\t..w.O..O.)...A.O
00000240   6D 7F D8 D0 9E 51 41 CB 99 5F 29 AB 9C 2E 18 62 9E F6 20 FA 94 87 C3 51 DB AE D2 82 2C 1F FB 56 BE 2E 08 3B   m....QA.._)....b.. ....Q....,..V...;
00000264   1A 4F C9 B1 7F 80 05 97 34 9D 7C BE F8 DE F9 36 46 0E B8 7F 28 20 B5 95 87 14 9D B5 7D AF CB CE 10 AE 1F 98   .O......4.|....6F...( ......}.......
00000288   B2 01 23 5D 88 8A A2 26 2E 5F 48 A1 7C 56 39 49 2E C4 B8 ED 2A F2 04 D1 4C 25 31 30 97 EB 37 0F 58 49 3A 7E   ..#]...&._H.|V9I....*...L%10..7.XI:~
000002AC   DA 1B 1E 2A 3C 32 82 EF A9 B1 7F B3 9D 27 76 F3 0F 44 35 9C 53 0F 63 79 5A AE F3 54 DA 56 D5 A1 92 17 34 CD   ...*<2.......'v..D5.S.cyZ..T.V....4.
000002D0   3C 2C D2 C6 F5 82 68 5B 2A 0C 47 7B 38 D8 BF BF 94 BB 67 75 1F 5A BE 40 83 BA 53 DE EE 4E 13 D6 3F E7 18 8A   <,....h[*.G{8.....gu.Z.@..S..N..?...
000002F4   ED 20 29 63 50 08 AE 55 9C 65 98 6E 9B 3F 31 5E 23 74 86 E5 58 97 82 3C BB 4A F0 6A 23 46 40 2A C8 94 28 09   . )cP..U.e.n.?1^#t..X..<.J.j#F@*..(.
00000318   40 94 00 29 44 D3 B0 F5 55 24 69 08 BD F0 88 FB F4 AA CA 64 DB 49 14 0F FB 7A 22 7B 89 D7 34 2C 91 E4 0B 3B   @..)D...U$i.........d.I...z"{..4,...;
0000033C   13 90 85 E2 4C 27 FE FB A9 3F 98 95 45 B8 2B 3E 38 F1 84 3C 75 DA 91 D9 36 12 28 08 93 BE 02 52 B1 F6 EC DD   ....L'...?..E.+>8..<u...6.(....R....
00000360   37 7F 5E 62 66 DB BA DA 3C 93 AD EE 26 AE 89 70 64 F7 9A BF BB 83 13 A9 C2 D6 0A 21 87 AB EA 14 3B 91 EC 8D   7.^bf...<...&..pd..........!....;...
00000384   1C 51 FE 56 B8 BE 57 8E 84 05 F3 FD E9 43 3B 24 00 D7 68 1A 0E D0 55 66 CC 3B F1 6F EC 8E 6F 99 78 74 19 52   .Q.V..W......C;$..h...Uf.;.o..o.xt.R
000003A8   68 7B 7A AB B7 EF D3 E0 BF BC 2F 2B 65 F2 B5 C9 8E 6E 59 2F 40 3A 28 DE 16 07 3C 61 DA 20 C4 4B 73 46 25 A4   h{z......./+e....nY/@:(...<a. .KsF%.
000003CC   5C 9D 10 47 17 41 65 51 3D 9C 3F 89 62 17 5C D2 5F 9D 75 3C 77 FD A4 69 C9 D4 4E 60 35 A3 3E B2 AD 1A E6 D5   \..G.AeQ=.?.b.\._.u<w..i..N`5.>.....
000003F0   41 BF 5B BD C1 C5 2B 1C 07 7C B1 2D 4D A7 D2 A9 CD 5B 63 3D C7 89 27 BF 6B C1 29 6B 1E 0F C2 0F B2 7C D8 63   A.[...+..|.-M....[c=..'.k.)k.....|.c
00000414   9A F0 BB 82 C6 6F C7 95 51 23 A7 FE F9 C8 6F CE 87 E0 19 BF 30 61 B5 6E E2 C3 54 12 5D 7D 7F 79 73 DF 7B 4C   .....o..Q#....o.....0a.n..T.]}.ys.{L
00000438   60 1A 94 00 14 1B C3 AA BB 0C 60 68 7F 1E D9 6D F6 4A 9E 4B 68 C7 43 E3 61 FA 70 1D 9B F8 34 1D FB 81 F1 46   `..........`h...m.J.Kh.C.a.p...4....F
0000045C   3E 68 C4 92 27 9D 0D 19 1C 8C AF 3E B1 C3 6A D7 AC 7A AD D7 0B D2 5F DF 50 04 73 25 0A 35 E7 4D 06 D7 DE 7C   >h..'.......>..j..z...._.P.s%.5.M...|
00000480   F3 64 DE 73 26 F7 37 23 F0 21 7A D2 6A 99 57 20 94 60 4A 19 49 60 5F FB 09 3C D1 C2 4E 8B 7A 76 A2 74 55 C0   .d.s&.7#.!z.j.W .`J.I`_..<..N.zv.tU.
000004A4   F6 9E 5D 76 C1 97 14 79 87 7E 44 7F 4D D3 ED B1 06 14 4F DE F6 BC 3D D8 EB 28 82 8A F4 FA 8D B9 51 87 14 2D   ..]v...y.~D.M.....O...=..(......Q..-
000004C8   0A 64 6A F6 F7 37 D3 A3 17 6A BF 6D 38 6C A8 35 9C EA 5F C3 12 85 B6 F0 5A C4 DB FA ED 5B 1B 5F EA C7 2A 8A   .dj..7...j.m8l.5.._.....Z....[._..*.
000004EC   92 A3 A4 13 40 FB 3F 67 37 D4 1D 29 35 37 CD ED 58 E4 A8 CF 2B 88 13 9D 38 65 6D 82 C5 41 A0 2A 20 53 3B AF   ....@.?g7..)57..X...+...8em..A.* S;.
00000510   22 ED 7B 9E AB 02 70 06 1F F1 98 F3 F0 F1 ED 8E F8 3C 01 E2 76 D1 77 0E E7 6C 68 09 97 0B 79 05 F8 A9 C9 49   ".{...p...........<..v.w..lh...y....I
```

ii. k=12 34 56 78 9A BC DE F0 , k1=12 23 45 55 67 78 88 88, k2=89 AA AB BA AC AE AD FA k


CrypTool 1.4.42 - DES (ECB) encryption of <startingexample-en>, key <12 34 56 78 9A BC DE F0>
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
startingexample-en
Starting example for the CrypTool version family 1.x (CT1)
DES (ECB) encryption of <startingexample-en>, key <12 34 56 78 9A BC DE F0>
Type here to search
57°F Sunny
ENG
1:52 AM
3/28/2022

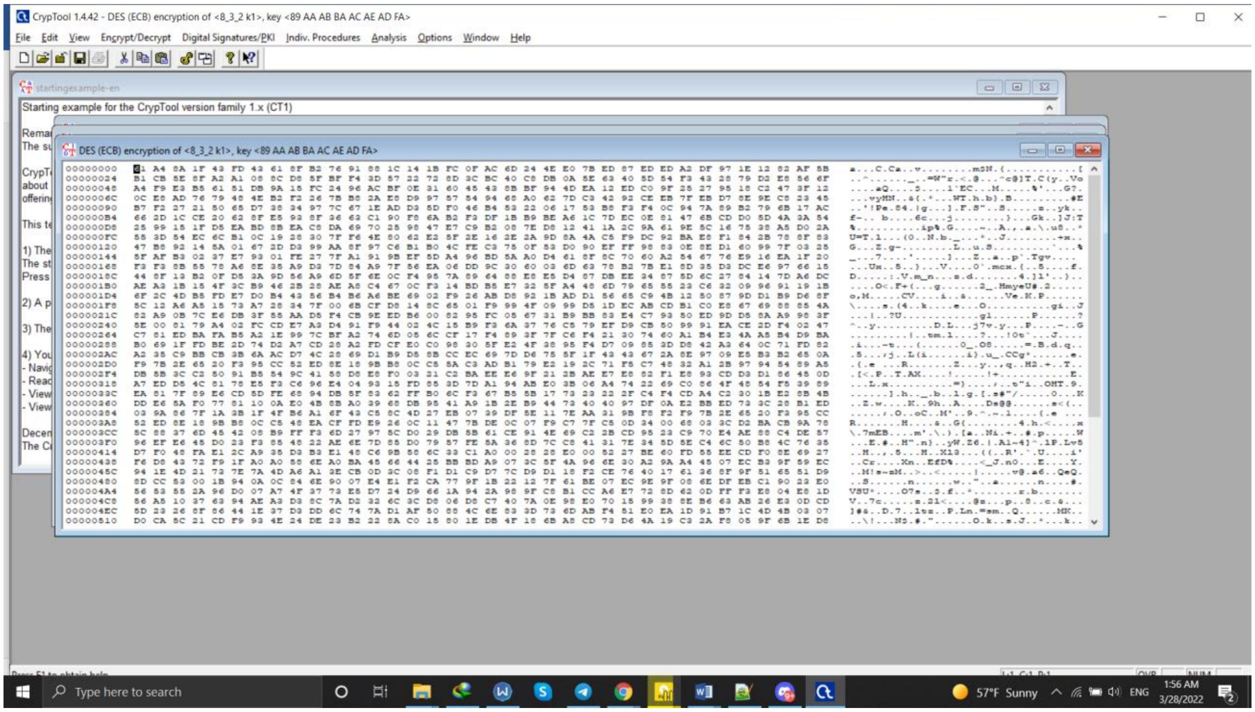
```
00000000  90 3B 63 14 A3 0F C8 37 E0 1D 94 98 39 38 C1 63 2F 4C 62 7A 4F 12 18 DA D4 96 A0 B0 A2 5E 27 92 9C 0E 19 50
00000024  96 53 44 27 4D 07 6F B2 2F 46 1F 16 DA C7 EA 42 30 3E 78 B5 02 E5 2E C2 57 D6 98 E9 1C 6C 20 98 2B DC DB 5A
00000048  E5 2A 93 9E 3B E6 69 78 F0 CD AB C7 C2 79 A6 2D B6 1C 48 E6 09 49 06 A5 24 5A 26 39 CC 84 13 64 5C F9 7D 89
0000006C  7B 13 53 6C 64 CF C0 C2 5E E2 19 DE A7 0A 4D 8A 05 BA 31 AA 7C 63 CF C2 A0 97 F0 9D 50 91 46 5D 1F F2 88 BA
00000090  0E 8C C1 12 81 F3 2C 19 B1 0B B8 33 D9 2D DF FA DB 54 39 C8 D3 FB 9F 96 A1 B0 42 9E C5 0F EC BC 13 FD 8F AE
000000B4  A2 82 05 21 6D 99 02 99 95 38 51 16 74 A5 D9 C1 0B 21 36 75 69 4F 24 38 FA AE 5D 10 27 7C E9 AC C5 86 97 74
000000D8  89 BA C5 F8 4D A4 4E B1 AA 03 EE 31 EA FC B2 AB 4F 66 55 17 26 F1 DD E0 27 4F 65 F0 85 37 34 37 5C 67 58 9A
000000FC  69 9D 9D DE 19 B7 A4 58 B4 2B 48 E3 3F D7 C1 DB 09 AD B2 4E C9 6C 1D 20 23 84 C3 37 B8 81 88 65 D6 59 BF 77
00000120  AC DE 99 15 F9 49 DC 63 A6 CA EB 65 29 CB 15 17 BB 58 17 0E 4C E2 52 96 80 52 36 07 C0 24 96 DE 29 9E A5 E8
00000144  71 11 F1 A0 60 2C 9D D8 68 F0 52 86 AA EC 03 AA 41 94 13 2E 89 16 F5 9D 74 0F 43 3C A3 2C 1C D2 36 93 8E 75
00000168  9C 10 94 A8 F4 BD 77 CB 3D A1 E0 75 B9 25 B5 CB A5 C6 1B 6F DE 7A 8E 68 BF 7E F9 E3 38 A4 E3 26 83 07 A2 38
0000018C  B8 76 D1 62 5E 6D 7E 12 60 3B FE 10 3A B3 D7 54 34 D2 B8 79 B5 74 26 D5 F6 CE 61 67 29 07 CA B9 D7 5C AC BD
000001B0  F8 38 4D 1B 48 35 D0 A0 42 28 7B EC C9 C7 CA 7E 81 F9 37 F8 60 7F E2 3A 3E AD 1E C5 0D 92 24 B9 02 CD A5 89
000001D4  D6 8A DA 94 A2 CE 36 44 18 CE FE 72 D2 CE 57 D6 BF 51 CD C8 64 B4 6F 55 76 CC 49 99 58 6E EC DE FF 44 FD 38
000001F8  FB F1 99 4D 0F F4 A7 FE 0E 64 53 F8 34 01 B7 7C 8F 6E 3A 89 1C CF 62 D9 97 34 42 3B CD 67 0A 3F 41 31 62 75
0000021C  02 7C D2 85 48 1C A5 E8 D8 D3 80 7D 3C E4 41 50 38 0E 0D E3 42 9A 6E 65 03 80 89 04 97 87 86 DF 1E A6 BC 14
00000240  75 2C BE 5D 1C F7 1D 83 19 63 D6 8C FA 38 91 27 D3 C6 98 8D 11 88 49 D4 FB 6E 54 F6 79 96 01 B0 6E 64 44 57
00000264  2A A1 90 08 00 EC 9E 06 C9 9A 2C 6C B6 1E 59 2D 8A 9F 9D E8 26 0E 2D E4 76 92 22 4A BD B4 92 66 D6 75 0B C5
00000288  5C BF 66 92 D8 83 23 B6 BA DD 0C 52 27 1E 33 2C FE 8C 93 D2 12 07 2F 69 90 FD EC 22 40 03 05 67 7E 84 43 7D
000002AC  D0 88 6A FE 74 72 52 F5 47 5B 5F 37 67 05 FE 28 7C 1F 2D 97 6A 00 E4 0A 67 DA 79 F9 CD FA 9C 5A 97 7C DB FC
000002D0  19 59 84 4B 18 7E 4D EA E0 BF 91 F0 DD 20 B8 89 06 60 C2 0E 1E 19 46 85 1D F9 58 8F 67 A1 5C B2 DD 27 F9 D1
000002F4  CE 00 D8 80 DA 2C D0 60 95 D2 5F DD B7 18 4B 6B 99 1D 27 71 87 9D A7 58 9A C7 2A 84 6A 80 8E 7E D2 B9 19 B8
00000318  3C 79 79 7A 9E 51 A5 06 A0 9B 4E CF 2A E4 23 28 F2 30 37 1A 00 1A 96 05 D0 5C F2 75 C0 FF 15 21 70 65 1E 10
0000033C  44 69 2A F7 41 64 18 35 65 59 83 A9 1E DA 0E 57 B4 F2 5A D6 3C 1B BE E9 E2 63 F6 86 FC CE 72 39 25 08 15 6C
00000360  14 E6 B0 BD 21 6B C0 62 D7 AB 4D 1D 2D 9D E0 8E 1C 72 6C 31 46 C0 1E 54 A5 96 01 CA F7 D8 BE 92 C9 8E BB B5
00000384  25 D1 D1 36 8D 96 6B 59 5A 40 39 2B BF F1 3B 01 3E 1F 05 98 EF 16 CD 4D DD 63 8B 28 19 59 84 4B 18 7E 4D EA
000003A8  E0 BF 91 F0 DD 20 B8 89 4D 4F 75 A0 5F 0B 60 BF D2 87 EB EB 10 C3 45 5B EF FB C0 F1 2D 90 07 4F E9 BD CE B1
000003CC  91 23 49 2C B8 C9 BD B6 F9 95 D6 7B 77 95 99 5E 7B FD 71 9A 8E 33 2C 42 4D 29 1D C2 99 D8 46 DA 2A A5 EA 7D
000003F0  C8 C4 28 2C C5 F9 7C D8 B3 96 A6 0A 78 67 E6 EE EE 86 6D DF BF A7 38 6F CA 99 BD DD AE 4E F1 90 D9 85 9D E6
00000414  F3 5C D7 DA E8 DB BB 2C E8 3B DB E5 D5 0D 13 37 E0 6C 45 B2 5F 6C 47 13 8E 33 C5 2D 1D 80 14 10 11 70 F9 74
00000438  FD 22 09 CF CC D5 84 1C 51 E5 7F 5C 83 07 B9 E1 46 07 7F 87 69 9B 4A B5 90 45 FD C8 07 6F B7 31 65 D5 79 E6
0000045C  C4 22 36 06 AB F7 50 D8 18 DB 66 F2 27 10 F6 87 BB F1 0A 4B ED 4E E7 BF 93 4A 4E C2 46 CF A0 B8 21 1B AC E2
00000480  A3 39 EB 37 B6 82 46 4D 6B 06 DE 04 18 55 F3 E8 E6 BB 82 52 12 88 6A 95 37 C5 B1 03 C8 FE C7 1A F4 CA 32 61
000004A4  7A 69 88 94 0B 1A 67 E5 A0 40 0B 9E FB D3 1D F6 64 40 D1 42 C8 25 E8 90 8C 9E 00 0D 2F 81 84 37 DB 80 FA D6
000004C8  CC C4 5C EE 85 B4 EB 48 64 59 E8 56 FD 5D 06 CC 3C 6F E5 48 D2 36 1E E9 7E A3 5D 31 21 5F FD 6E 56 32 8B 5B
000004EC  46 C1 51 A1 E5 28 05 81 AC 14 FE 44 18 BC 28 B7 47 5F 3E AC 43 DB 69 FA 01 07 49 4C 6C 07 71 48 C2 2B 9A C4
00000510  E0 27 2F 9A 38 E5 35 8A 3A E5 15 8E F4 8F 42 82 4A B0 01 D4 4D 55 B7 97 9D AD 99 14 E9 8A 58 FE 94 27 AE B6
```

k1


CrypTool 1.4.42 - DES (ECB) encryption of <8_3_2 k>, key <12 23 45 55 67 78 88 88>
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
startingexample-en
Starting example for the CrypTool version family 1.x (CT1)
DES (ECB) encryption of <8_3_2 k>, key <12 23 45 55 67 78 88 88>
Type here to search
57°F Sunny
ENG
1:54 AM
3/28/2022

```
00000000  FB 65 01 E0 2A 31 4B 8A 3C 5C 16 64 89 2A ED BC DF 1D E6 82 BF 5C B2 F1 F5 8C B7 81 AE 91 1E 2B 99 09 BB 4F
00000024  7B C2 FA 1E 81 8D 86 EC 8C 82 C2 E7 3F BF D3 F7 CF 54 39 76 B2 CE 0C C2 DC 8B 39 89 EE AA CB 04 3C 27 1E DA
00000048  15 09 D0 9C AF A6 26 4C 84 80 4B C4 66 61 21 BC 2D AA 88 D8 C9 7D 12 8D 2E 64 98 4A A3 0F 46 64 DD 38 CF A9
0000006C  27 2F 71 DA 76 DD 13 42 3E D2 60 AF E1 13 E7 2F 8D 21 81 F0 E6 1A 15 64 03 1A D0 1E D3 AC D1 20 18 E6 DF BD
00000090  E2 DC 1B 90 0D A2 13 18 1F 12 83 1B 39 F3 2B 0E B4 B6 8E 5C 4B B7 3A FB 3A A8 3D E2 F4 D0 7F 6F 9B 2B 1F C9
000000B4  3C 2A 64 B5 6C E3 39 3E BB 55 DA CA 6B F4 5B 67 D5 C2 D5 87 43 9A C5 68 9C 76 67 9A D2 62 50 D8 5E DB 9F 96
000000D8  BF 32 45 1E 9F 5C 70 F8 A2 F6 FB BB 0B 6D 19 FA 70 84 60 EF 75 44 74 41 BE 0E 7A 0F 7B 54 91 1F F2 9C 8C 3E
000000FC  CD 82 90 93 FC D3 9B AB 93 57 70 DC FB 38 73 17 E2 40 72 EB 1D 88 D7 9A F8 AC B3 CE A5 0F 74 9D BE 7F 65 0C
00000120  9B AC 08 E9 4F 66 D2 6A 81 28 65 EF A4 D5 21 AF 60 F4 0A 58 0F 20 B3 65 F7 46 BD FF 4F 33 B8 59 5E 38 6D A0
00000144  44 84 49 1F 65 65 EC 26 CB 20 3E EE AE 3B 09 69 1C 0D 34 44 8F 1C C7 E2 FF 78 2B D7 6F 63 AC 2A CB 8F 09 F9
00000168  15 F1 5B 01 D2 0D 2C C4 3F AF F3 FD 51 3D CA CF BF 44 66 1D 10 CA 2C DA 8D EC 63 7A 7B A2 98 C2 B8 37 AA 76
0000018C  34 27 F2 E2 B4 62 BC 99 00 42 7C AA 87 40 43 9F 32 53 10 80 EB 61 1C D7 7D 3D C2 0D 67 0F FF 9B E0 8E 56 44
000001B0  63 C6 D3 C5 A2 E3 C5 18 31 2B 73 CB FC 7E 43 D2 70 54 AD D8 39 09 DE 4A C1 04 4E 60 9E D9 F4 09 C8 B7 1C 51
000001D4  64 6A 87 61 7A 18 4E 94 8F 0A C9 DC D9 81 2E 72 81 AC A8 0A EE 36 C5 76 73 D8 85 68 C1 8C 7C 1A F9 7F C6 BC
000001F8  97 8D 7C 43 BC FE 8D 33 F8 56 40 46 E1 47 91 23 22 9D BB 53 34 FF CD 02 DE 06 DF 8D 7B E1 01 40 73 41 DE 10
0000021C  A6 49 02 70 27 D9 E7 82 58 97 FE 1C 85 F5 7F D1 94 FF 13 C6 7E 2F 16 03 D5 19 36 C9 B5 33 A1 70 F3 7D 64 8D
00000240  B0 04 7B E1 91 15 7B 5A D7 CF 6E 5A 2F 46 5C 7A EC 6C FB FD 6C 6B 86 9E C4 C9 9E A9 A0 94 2F 69 65 6D 83 F9
00000264  17 3C 45 C2 B8 30 27 04 95 1D 88 67 F4 6D 1C 87 D9 D1 8E 2A 91 18 1E 71 56 4F FD 17 F8 06 83 04 BD 89 D8 B5
00000288  5C 6A 88 4E 35 B6 B3 6C DF 79 01 98 D3 07 B3 AB FE 73 1F 29 C4 97 6E 66 A2 23 3E 68 BE 93 12 5C 69 24 DB E0
000002AC  29 83 7B 64 52 36 05 55 16 CC EE 13 CB E2 E0 F8 0E 07 30 FE 9A ED A6 DA 1D 09 10 87 59 22 7F 7B AF 40 E6 FE
000002D0  72 86 52 17 B2 23 E6 4B A1 87 C1 81 E5 6B 7D 62 33 2E 80 8F B9 B4 3C 5D FF 8E B4 59 24 8A 20 08 68 B2 22 90
000002F4  6E 93 8F B9 09 76 3A 75 EC E3 A4 01 91 34 00 32 A0 1E D0 2D 26 A1 4E A3 60 89 2A 03 0C 98 85 8A 0E 27 58 8A
00000318  39 EC D9 BB 2A F4 42 98 26 DF B2 26 AD A4 74 5D 24 77 00 E3 63 45 CF B1 DD D8 C7 6C D2 04 D7 A2 78 70 4E 10
0000033C  C2 0B C8 EC EE 90 D5 6F 0A 9D 54 C0 29 4B 43 14 20 39 03 2A E4 0E 45 F1 7F 5E B9 8C 5C 1A 5C AE DC C8 FB B7
00000360  A3 E1 3E 71 2D 35 CC 6D 56 BC 33 74 F5 34 AA 72 AD 74 36 25 AB 37 AF CE 74 7C BB 08 CA A8 0E 56 98 89 5A 86
00000384  36 2D 6A 1A 1B DF DA BA A6 8A CA 30 BA C4 14 7A F4 67 C3 AD 23 3E 4E 06 EA 70 2E 17 72 86 52 17 B2 23 E6 4B
000003A8  A1 87 C1 81 E5 6B 7D 62 FC 06 2D 70 0C 83 C9 3E 90 51 B6 B6 C9 48 42 03 4C A3 9B 91 C5 A5 D9 AE 27 44 F7 62
000003CC  28 B7 96 B3 66 9B 8E 15 3D C7 EE 40 F8 17 DF 9A D4 4E FE 8C 3F C3 BD 06 8F A2 D3 89 C2 E6 D3 56 22 D8 B3 2A
000003F0  47 B6 F0 15 D7 41 95 0A C7 C4 FB 28 23 CB A1 79 18 EB 34 59 2F 96 1B 3D 75 A4 43 B6 B3 CB F5 C5 15 A8 72 AD
00000414  A8 AF 77 2A 75 29 5E A5 A5 7E 96 9E 63 0A B8 DF 19 24 55 A6 44 64 87 3A E5 7E 6C 85 63 41 82 D1 68 FA 5D F9
00000438  5D C5 9D 58 6F E2 76 3F 15 52 EC FB 4D 86 7A 7A 90 9D 89 63 BA 4C 35 7A CE BA 1A D5 F8 B1 47 8C 83 57 88 13
0000045C  D8 17 CC 8A 8A 68 0D BF 98 13 AE B6 38 66 90 31 76 AA D0 80 F4 9E 52 9C C9 89 2E 74 4D 72 60 9B D5 78 CE B2
00000480  44 B9 0D D9 0E 48 91 FA C9 70 CE DF A4 18 6A 3A 3D 63 FB 08 39 D9 40 31 08 C2 7C A5 7A EE E0 A4 0F 03 61 9F
000004A4  1F 82 73 6E CF 19 52 B9 89 3C A2 35 74 A9 D9 3A 60 16 A8 21 A3 3A 57 F2 97 16 70 3C 68 4C B7 B3 16 10 2D EA
000004C8  18 49 9B FE 0C 19 16 53 69 07 D6 DA 62 99 56 62 C2 51 54 10 8D 21 93 12 A0 08 81 AE FF DB F5 6F A8 F5 B2 BF
000004EC  F0 56 37 98 5E 92 B8 20 34 57 93 68 02 10 24 35 4F 70 2A 99 15 C5 9D 27 0D 94 3D 58 97 EA 9C 40 BC 62 AF C9
00000510  35 27 5A 7A E3 58 B1 A0 7F 7D B4 52 DF 42 13 62 AE 14 84 CD 4A 2C 32 83 DD 25 B9 F9 4F 24 F7 32 DE BC 40 3D
```

k3



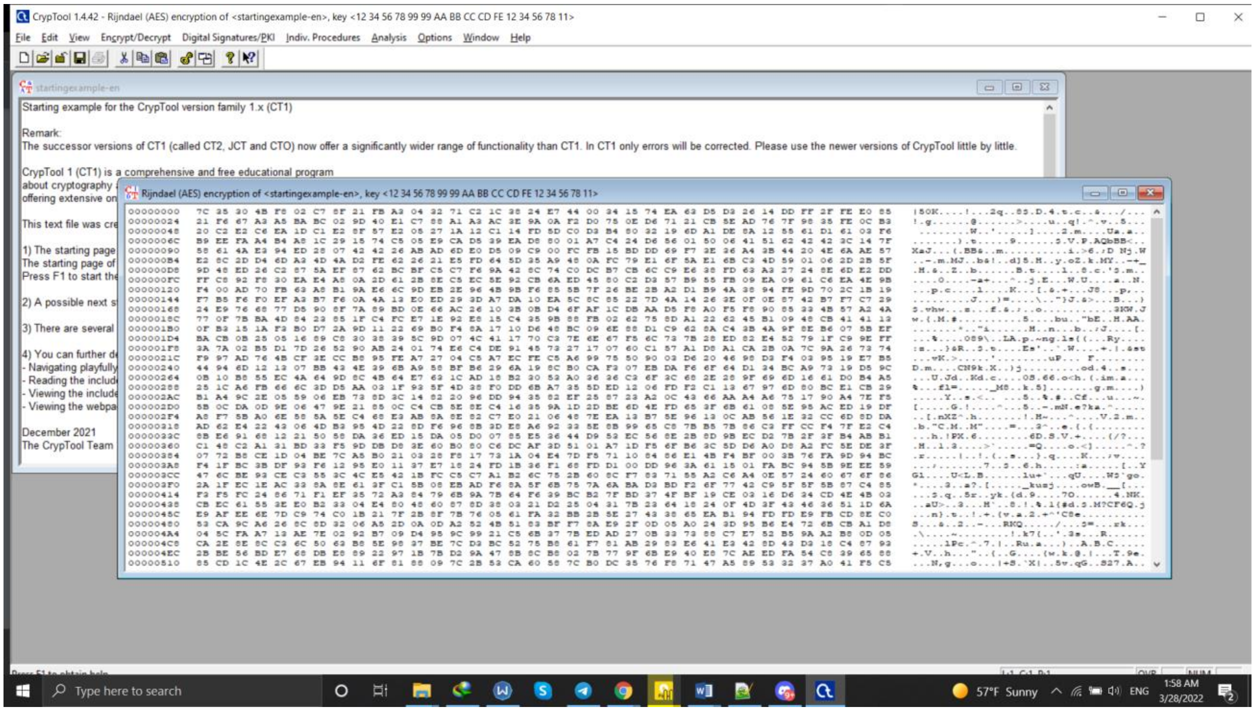
CrypTool 1.4.42 - DES (ECB) encryption of <8_3_2 k1>, key <89 AA AB BA AC AE AD FA>

DES (ECB) encryption of <8_3_2 k1>, key <89 AA AB BA AC AE AD FA>

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

## 8.4 :

key : 12 34 56 78 99 99 AA BB CC CD FE 12 34 56 78 11



CrypTool 1.4.42 - Rijndael (AES) encryption of <startingexample-en>, key <12 34 56 78 99 99 AA BB CC CD FE 12 34 56 78 11>

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.

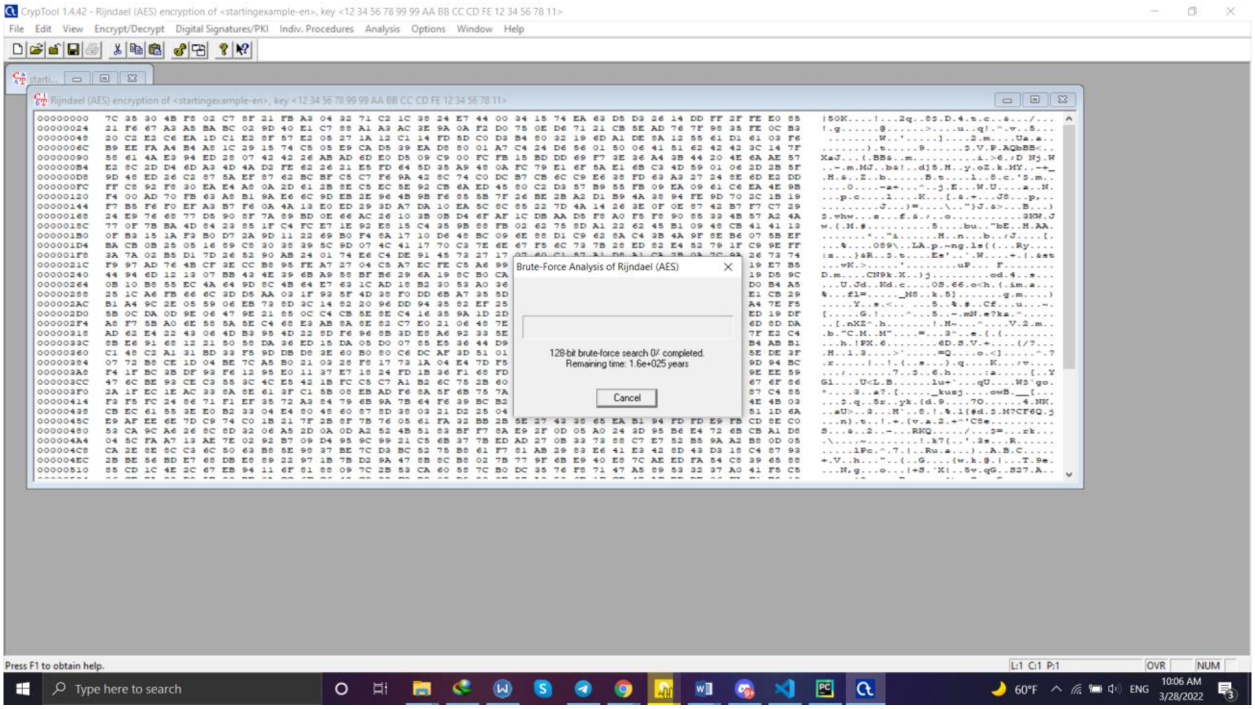
CrypTool 1 (CT1) is a comprehensive and free educational program

December 2021
The CrypTool Team

Rijndael (AES) encryption of <startingexample-en>, key <12 34 56 78 99 99 AA BB CC CD FE 12 34 56 78 11>

## 8.5 :

i)



CrypTool 1.4.42 - Rijndael (AES) encryption of <startingexample-en>, key <12 34 56 78 99 99 AA BB CC CD FE 12 34 56 78 11>

Brute-Force Analysis of Rijndael (AES)

128-bit brute-force search 0% completed.
Remaining time: 1.6e+025 years

ii) in this part we get the answer immediately