Understanding Cryptography

Answers of Homework No.2

فصل سوم

1.

حل:

1.1.

به ازای هر x داریم: $DES_k(x) = DES_k^{-1}(x)$

در این جا باید عمل رمزنگاری و رمزگشایی یکسان باشد. ترتیب کلیدهای مورد استفاده در رمزنگاری به صورت $(k_1, k_2, k_3, \dots \dots, k_{16})$ است و ترتیب کلیدهای مورد استفاده در رمزگشایی به صورت $(k_{16}, k_{15}, \dots, k_1)$ است. پس نتیجه می‌شود که زیرکلیدهای تولید شده باید دارای رابطه زیر با یکدیگر باشند:

$$k_{i+1} = k_{16-i} \quad for\ i = 0,1, \dots \dots ,7$$

1.2.

DES دارای ۴ عدد $weak\ keys$ از نوع ۶۴ بیتی است. طبق نکته قسمت قبل برای اینکه شیفت بیت ها اثری نداشته باشد لذا داریم:

Keys before parities drop (64 bits)
0101 0101 0101 0101
1F1F 1F1F 0E0E 0E0E
E0E0 E0E0 F1F1 F1F1
FEFE FEFE FEFE FEFE

Actual key (56 bits)
0000000 0000000
0000000 FFFFFFF
FFFFFFF 0000000
FFFFFFF FFFFFFF

1.3.

به طور کلی احتمال انتخاب یکی از این کلیدهای ضعیف به طور تصادفی برابر است با:

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

1.4.

کلیدهای ضعیف نباید در $key\ \ generation$ استفاده شوند. به دلیل اینکه این کلیدها به راحتی شکسته می شوند و فضای این کلیدها بسیار محدود می باشد.

1.5.

به طور کلی ۶ زوج (جفت) یا ۱۲ عدد کلید $semi\ weak$ وجود دارد.

$$01FE\ \ 01FE\ \ 01FE\ 01FE\ \ \ and\ \ \ FE01\ \ FE01\ \ FE01\ \ FE01$$
$$1FE0\ \ 1FE0\ \ 0EF1\ \ 0EF1\ \ \ and\ \ \ E01F\ \ \ E01F\ \ \ F10E\ \ \ F10E$$
$$01E0\ \ 01E0\ \ 01F1\ \ 01F1\ \ and\ \ E001\ \ \ E001\ \ \ F101\ \ \ F101$$
$$1FFE\ \ 1FFE\ \ 0EFE\ \ 0EFE\ \ and\ \ \ FE1F\ \ \ FE1E\ \ FE0E\ \ \ FE0E$$
$$011F\ \ 011F\ \ 010E\ \ \ 010E\ \ \ and\ \ 1F01\ \ 1F01\ \ 0E01\ \ 0E01$$
$$E0FE\ \ E0FE\ \ F1FE\ \ \ F1FE\ \ and\ \ \ FEE0\ \ FEE0\ \ FEF1\ \ FEF1$$

1.6.

DES دارای کلید $semi\ weak$ است که تنها دو زیرکلید متفاوت تولید می‌کنند که هر کدام به تعداد ۸ مرتبه در الگوریتم استفاده می شوند.

1.7.

DES دارای 2^{56} کلید است. تعداد کل کلیدهای ممکن ۶۴ عدد می باشد که ۴ عدد $weak$ ، ۱۲ عدد $semi\ weak$ و ۴۸ عدد $possible\ weak\ key$ هستند. احتمال انتخاب یکی از این کلیدها تقریبا ناممکن است. به این ترتیب داریم:

احتمال $weak$ برابر است با : $\frac{2^2}{2^{56}}$

احتمال $semi\ weak$ برابر است با: $\frac{12}{2^{56}}$

احتمال $possible\ weak\ key$ برابر است با : $\frac{48}{2^{56}}$

احتمال مجموع برابر است با : $\frac{4+12+48}{2^{56}}$

1.

حل :

2.1.

یک ویژگی مهم که DES را امن می سازد غیر خطی بودن $S-BOX$ها است که باعث $confusion$ می‌شود. در واقع با روش های خطی نمی توان آن ها را شکست.

2.2.

$$S_1(x_1) \oplus S_1(x_2) \neq S_1(x_1 \oplus x_2)$$

$$S_1(101010_2) \oplus S_1(010101_2) \neq S_1(101010_2 \oplus S_1 010101_2)$$
$$0110_2 \oplus 1100_2 \neq S_1(111111_2)$$

$$1010_2 \neq 1101_2$$

2.3.

اگر ما اولین و ششمین بیت را با هم بنویسیم، در حالت باینری11 را داریم. که معادل ۳ است و نشاندهنده شماره سطر است. بیت های باقیمانده در حالت باینری برابر 0001 هستند که معادل ۱ است و نشاندهنده شماره ستون است پس ما مقدار سطر سوم و ستون یکم را در جدول جست و جو می کنیم. که برابر 12 در دسیمال است. که مقدار باینری آن برابر 1100 است. پس ورودی 100011 خروجی 1100 را بدست می‌دهد.

3.

حل:

3.1.

در مرحله اول یا مرحله عبور از $initial\ permutation$ اگر x متن اصلی باشد، به دلیل اینکه بیت ۵۷ ام در متن اصلی ۱ است داریم: $(x = 0000 \ldots \ldots 010 \ldots .0)$.
$IP(x)$ بیت ۵۷ را به بیت ۳۳ نگاشت می دهد یعنی همه بیت ها صفر شده و فقط بیت ۳۳ام برابر ۱ می‌شود و وارد دور شماره یک می گردد. پس $L_0 = 0$ (۳۲ بیت) و $R_0 = 1000 \ldots .0$ (۳۲ بیت) است. حال R_0 وارد تابع f شده موقع حساب کردن $f(R_0)$ می‌توانیم کلید صفر را به دلیل اینکه $(a \oplus 0 = a)$ است به حساب نیاوریم. پس در نتیجه کلید هم صفر است پس نتیجه XOR هم تغییری نمی‌کند. یعنی $(x \oplus k = 0) = x$
در مرحله $expansion$، $E(R_0)$ بیت اول R_0 را به بیت دوم و ۴۸ ام نگاشت می‌دهد. این یعنی مقادیر S_{2-7} در ورودی همه ۰ می گیرند.S_1 در ورودی دارای مقدار 010000_2 است و S_8 مقدار 000001_2 را می‌گیرد.

3.2.

با عبور ورودی ها از $s - box$ خروجی های زیر طبق جدول کتاب حاصل می شود.

	S1	S2	S3	S4	S5	S6	S7	S8
ورودی	010000	000000	000000	000000	000000	000000	000000	000000
سطر متناظر	$00 = 0$	$00 = 0$	$00 = 0$	$00 = 0$	$00 = 0$	$00 = 0$	$00 = 0$	$01 = 1$
ستون متناظر	$1000 = 8$	$0000 = 0$	$0000 = 0$	$0000 = 0$	$0000 = 0$	$0000 = 0$	$0000 = 0$	$0000 = 0$
خروجی	0011	1111	1010	0111	0010	1100	0100	0001

بعد از عملیات $permutation$ روی خروجی $s-box$ داریم:

$$R_1 = 1101\ 0000\ 0101\ 1000\ 0101\ 1011\ 1001\ 1110_2$$

این مقدار سپس با L_0 ، XOR شده تا مقدار R_1 را تولید کند. این گام متوقف شده چون مقدار L_0 صفر است. مقادیر محاسبه شده L_1 و R_1 به شرح زیر است:

$$L_1 = R_0 = 08000000_{16}$$
$$R_1 = D0585B9E_{16}$$

3.3.

مینیمم تعداد بیت‌های خروجی (در هر $S-BOX$) که در نتیجه یک بیت تغییر در ورودی تغییر خواهد کرد برابر ۲ است.

3.4.

در حالتی که $plaintext$ کاملا صفر است با توجه به این‌که همه‌ی بیت‌های ورودی صفر تفاوتی در $IP(x)$ ایجاد نمی‌کنند خروجی به صورت زیر است:

$$L_0 = R_0 = 0$$

	S1	S2	S3	S4	S5	S6	S7	S8
ورودی	000000	000000	000000	000000	000000	000000	000000	000000
خروجی	1110	1111	1010	0111	0010	1100	0100	1101

بعد از عملیات $permutation$ داخلی تابع f و XOR نمودن با L_0 داریم:

$$R_1 = 1101\ 0000\ 0101\ 1000\ 0101\ 1011\ 1001\ 1110_2$$
$$L_1 = 0$$

به طور کلی زمانی که همه بیت ها صفر باشند خروجی 10110001101100011010111011100 است و موردی که قبلا محاسبه شده بود برابر 11010000010110000101101110011110 است. حاصل XOR نمودن این دو مقدار 00001000100000001000000000100010 است که نشان دهنده تغییر ۵ بیت است به دلیل اینکه L_1 مستقیما وارد R_0 شده و یک بیت از L_1 نیز ۱ است، مجموعا دیده می‌شود به ازای تغییر ۱ بیت در ورودی ۶ بیت با هم تفاوت دارند.

فصل چهارم

۴.

حل :

Feedback kindly provided by Lisa Roy in the comment section has allowed me to correct some errors in earlier versions of this answer. Given that we have now converged upon a common answer, I can be reasonably sure of correctness.

Note: From now on the state is represented as a 4x4 grid of bytes expressed in hexadecimal. This makes other transformations easier to represent also. The ordering of the bytes within the grid is as follows:

A_0	A_4	A_8	A_{12}
A_1	A_5	A_9	A_{13}
A_2	A_6	A_{10}	A_{14}
A_3	A_7	A_{11}	A_{15}

1. This question is slightly confusingly expressed and it took me a while to figure out what is meant. The keys k_0 and k_1 are given as a single array $(W_0, \ldots, W_7)$. In fact, $k_0 = W_0, \ldots, W_3$ and $k_1 = W_4, \ldots, W_7$. As such the first step is the initial k_0 key adition which occurs before we get into applying the rounds. The first word of the input is the only one that isn't all-zeroes. As such, the state after k_0 addition is:

> *Note*: From now on the state is represented as a 4x4 grid of bytes expressed in hexadecimal. This makes other transformations easier to represent also.
>
> | | | | |
> |---|---|---|---|
> | $2A$ | 28 | AB | 09 |
> | $7E$ | AE | $F7$ | CF |
> | 15 | $D2$ | 15 | $4F$ |
> | 16 | $A6$ | 88 | $3C$ |
>
> It's worth noting that the four columns correspond exactly to the $k_0 = (W_0, \ldots, W_3)$ subkey bytes with the exception of the first cell, which was slightly altered by the XOR operation.
>
> After applying the ByteSubstitution (S-box) layer, the state is as follows:
>
> | | | | |
> |---|---|---|---|
> | $E5$ | 34 | 62 | 01 |
> | $F3$ | $E4$ | 68 | $8A$ |
> | 59 | $B5$ | 59 | 84 |
> | 47 | 24 | $C4$ | EB |
>
> The ShiftRows layer is a very simple transformation. The first row remains unchainged. The other rows are rotated right by a number of positions; the second by 3, the third by 2 and the fourth by 1. This gives the following:

$E5$	34	62	01
$E4$	68	$8A$	$F3$
59	84	59	$B5$
EB	47	24	$C4$

The final transformation (other than the k_1 addition) is the MixColumn layer. This involves a Galois Extension Field matrix multiplication with the following description:

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

The C values refer to the outputted column. The B values refer to the input columns which were the output of the ShiftRows layer. The indexes here are preserved from prior to the shift. Each new column can be calculated left-to-right using this procedure.

it should also be noted that 03 here would refer to $x + 1$ in $GF(2^8)$. The same logic is used to turn a hex byte into a Galois Extension Field polynomial. The reduction polynomial is the AES primitive polynomial:

$$P(x) = x^8 + x^4 + x^3 + x + 1$$

As such the calculation to be performed is as follows for each of the columns:

$$\begin{pmatrix} 02 \times E5 + 03 \times E4 + 01 \times 59 + 01 \times EB \\ 01 \times E5 + 02 \times E4 + 03 \times 59 + 01 \times EB \\ 01 \times E5 + 01 \times E4 + 02 \times 59 + 03 \times EB \\ 03 \times E5 + 01 \times E4 + 01 \times 59 + 02 \times EB \end{pmatrix}$$

$$\begin{pmatrix} 02 \times 34 + 03 \times 68 + 01 \times 84 + 01 \times 47 \\ 01 \times 34 + 02 \times 68 + 03 \times 84 + 01 \times 47 \\ 01 \times 34 + 01 \times 68 + 02 \times 84 + 03 \times 47 \\ 03 \times 34 + 01 \times 68 + 01 \times 84 + 02 \times 47 \end{pmatrix}$$

$$\begin{pmatrix} 02 \times 62 + 03 \times 8A + 01 \times 59 + 01 \times 24 \\ 01 \times 62 + 02 \times 8A + 03 \times 59 + 01 \times 24 \\ 01 \times 62 + 01 \times 8A + 02 \times 59 + 03 \times 24 \\ 03 \times 62 + 01 \times 8A + 01 \times 59 + 02 \times 24 \end{pmatrix}$$

$$\begin{pmatrix} 02 \times 01 + 03 \times F3 + 01 \times B5 + 01 \times C4 \\ 01 \times 01 + 02 \times F3 + 03 \times B5 + 01 \times C4 \\ 01 \times 01 + 01 \times F3 + 02 \times B5 + 03 \times C4 \\ 03 \times 01 + 01 \times F3 + 01 \times B5 + 02 \times C4 \end{pmatrix}$$

This produces the following state:

54	13	$3C$	$7D$
36	34	$A2$	FC
95	86	36	$D4$
44	$3E$	$3D$	$D6$

All that's left to do after this is the KeyAddition layer for $k_1 = W_4, \ldots, W_7$:

$F4$	$9B$	$1F$	57
CC	60	01	90
$6B$	AA	$0F$	$A2$
53	$8F$	04	$D3$

Therefore, the output of the first round of encryption is as follows (remembering to read it out column-wise):

$$F4CC6B539B60AA8F1F010F045790A2D3_{16}$$

2. For the case that the input is all-zeroes, the state after the k_0 key addition will be as follows (only the first byte is different from part 1):

$2B$	28	AB	09
$7E$	AE	$F7$	CF
15	$D2$	15	$4F$
16	$A6$	88	$3C$

After applying the ByteSubstitution (S-box) layer, the state is as follows:

$F1$	34	62	01
$F3$	$E4$	68	$8A$
59	$B5$	59	84
47	24	$C4$	EB

After applying the ShiftRows layer, the state is as follows:

$F1$	34	62	01
$E4$	68	$8A$	$F3$
59	84	59	$B5$
EB	47	24	$C4$

Up until this point, only one byte (in fact only one bit) has been altered in compared to part 1. The MixColumn introduces some diffusion, and after this layer is applied, the state is as follows:

$7C$	13	$3C$	$7D$
22	34	$A2$	FC
81	86	36	$D4$
78	$3E$	$3D$	$D6$

The first column of the state now has a different set of values than in part 1, the others are unaltered. All that's left to do after this is the KeyAddition layer for $k_1 = W_4, \ldots, W_7$:

The first column of the state now has a different set of values than in part 1, the others are unaltered. All that's left to do after this is the KeyAddition layer for $k_1 = W_4, \ldots, W_7$:

$F4$	$9B$	$1F$	57
CC	60	01	90
$6B$	AA	$0F$	$A2$
53	$8F$	04	$D3$

Therefore, the output of the first round of encryption is as follows (remembering to read it out column-wise):

$$DCD87F6F9B60AA8F1F010F045790A2D3_{16}$$

3. We can see how many output bits have been altered by XORing the two output values together. This produces:

$$2814143c00000000000000000000000_{16}$$

In this form, we can clearly see that only the first column is altered after the first round.

$$2814143c_{16} = 10100000010100000101000011110_2$$

The 1s in the binary above correspond to output bits which have changed. There are ten of them, so therefore the number of output bits which have changed due to a 1 bit change in input, in this instance, is 10 after the first round. The ShiftRows operations in further rounds will diffuse this effect to other columns.

5.

حل:

$$\forall\, a_i \in \ GF(2) = \{0,1\} : p(x) = a_4x^4 + a_3x^3 + a_2x^2 + a_1x^1 + a_0$$

هدف ما یافتن $P(x)$ های درجه ۴ است در نتیجه $a_4 = 1$. هم‌چنین باید در نظر داشته باشیم چندجمله‌ای مورد نظر باید $irreducible$ باشد یعنی در $GF(2)$ ریشه نداشته باشد. یعنی $p(0) \neq 0$ و $p(1) \neq 0$.

$$p(0) \neq 0 \ \rightarrow \ \ a_0 \neq 0 \rightarrow a_0 = 1$$

$$p(1) \neq 0 \ \rightarrow \ \ 1 \times 1 + a_3 + a_2 + a_1 + 1 \neq 0 \quad \rightarrow a_3 + a_2 + a_1 \neq 0 \ \ mod\ 2$$

البته می توان گفت اگر a_0 یک نباشد چند جمله ای irreducible نیست چون در $p(x)$ از xهای آن می‌توان فاکتورگیری کرد و به ۲ عبارت با درجه کمتر قابل تقسیم است.

بنابراین 4 حالت داریم:

$$a_3 = 1, a_2 = 1, a_1 = 1 \ \ \rightarrow \mathrm{p(x)} = x^4 + x^3 + x^2 + x^1 + 1 \ \ \surd$$
$$a_3 = 1 \ \ \rightarrow \mathrm{p(x)} = x^4 + x^3 + 1 \ \ \surd$$
$$a_1 = 1 \ \ \rightarrow \mathrm{p(x)} = x^4 + x + 1 \ \ \surd$$
$$a_2 = 1 \ \ \rightarrow \mathrm{p(x)} = x^4 + x^2 + 1 \ \ \times$$

چند جمله ای آخر تحویل پذیر است یعنی داریم:

$$\mathrm{p(x)} = x^4 + x^2 + 1 \ \ mod\ 2 = (x^2 + x + 1)^2$$

در نتیجه سه چندجمله ای دیگر چون به هیچ کدام از عوامل درجه پایین‌تر خود تجزیه نمی‌شوند $irreducible$ هستند.

به طور کلی سه چندجمله ای $irreducile$ در $GF(2)$ از درجه ۴ وجود دارد.

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

6.

حل:

×	۰	۱	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	0	0	0	0	0	0	0
1	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
x	0	x	x^2	x^2+x	$x+1$	1	x^2+x+1	x^2+1
$x+1$	0	$x+1$	x^2+x	x^2+1	x^2+x+1	x^2	1	x
x^2	0	x^2	$x+1$	x^2+x+1	x^2+x	x	x^2+1	1
x^2+1	0	x^2+1	1	x^2	x	x^2+x+1	$x+1$	x^2+x
x^2+x	0	x^2+x	x^2+x+1	1	x^2+1	$x+1$	x	x^2
x^2+x+1	0	x^2+x+1	x^2+1	x	1	x^2+x	x^2	$x+1$

به دلیل اینکه $p(x) = x^3 + x + 1$ یک چند جمله ای درجه ۳ است پس در $GF(2^3)$ یک جدول 8×8 داریم. در واقع از ۰۰۰ تا ۱۱۱ داریم. باید چند جمله ای های مربوط به هر کدام را بنویسیم. روش به دست آوردن سطر و ستون قرمز رنگ جدول بالا در اینجا بیان شده است.

$$000 = 0$$
$$001 = 1$$
$$010 = x$$
$$011 = x + 1$$
$$100 = x^2$$
$$101 = x^2 + 1$$
$$110 = x^2 + x$$
$$111 = x^2 + x + 1$$

به این ترتیب بعد از به دست آوردن چند جمله‌ایهای بالا هر دو چندجمله ای را در $mod\ p(x)$ ضرب می‌کنیم سپس ضرایب چند جمله ای به دست آمده را به $mod\ 2$ حساب نموده و در نهایت باید چند جمله‌ای را به $mod\ p(x)$ حساب نمود. البته باید در نظر داشت محاسبات در $GF(2)$ صورت می پذیرد یعنی اگر در چند جمله ای ضریب -1 داشتیم با $+1$ برابر است.

روش به دست آوردن عناصر جدول:

به طور مثال چند نمونه در اینجا توضیح داده شده است:

$$(x^2+1)(x) = x^3+x \mod(2) = x^3+x \mod p(x) = -1 \text{ in } GF(2) = 1$$
$$(x^2+1)(x+1) = x^3+x^2+x+1 \mod(2) = x^3+x^2+x+1 \mod p(x) = x^2$$

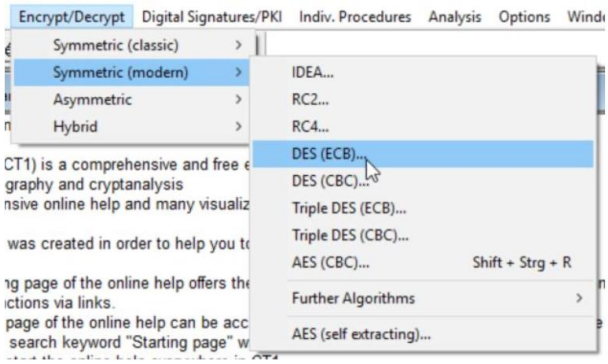
$$(x^2+1)(x^2+1) = x^4+2x^2+1 \mod(2) = x^4+1 \mod p(x) = -x^2-x-1 \text{ in } GF(2) = x^2+x+1$$

$$(x^2+1)(x^2) = x^4+x^2 \mod(2) = x^4+x^2 \mod p(x) = -x \text{ in } GF(2) = x$$
$$(x^2+x)(x+1) = x^3+2x^2+x \mod(2) = x^3+x \mod p(x) = 1$$
$$(x^2+x+1)(x+1) = x^3+2x^2+2x+1 \mod(2) = x^3+1 \mod p(x) = x$$
$$(x^2+x+1)(x^2) = x^4+x^2+x^3 \mod(2) = x^4+x^2+x^3 \mod p(x) = -2x-1 \mod 2 = -1 \text{ in } GF(2) = 1$$
$$(x^2+x)(x^2+x) = x^4+2x^3+x^2 \mod(2) = x^4+x^2 \mod p(x) = -x \text{ in } GF(2) = x$$

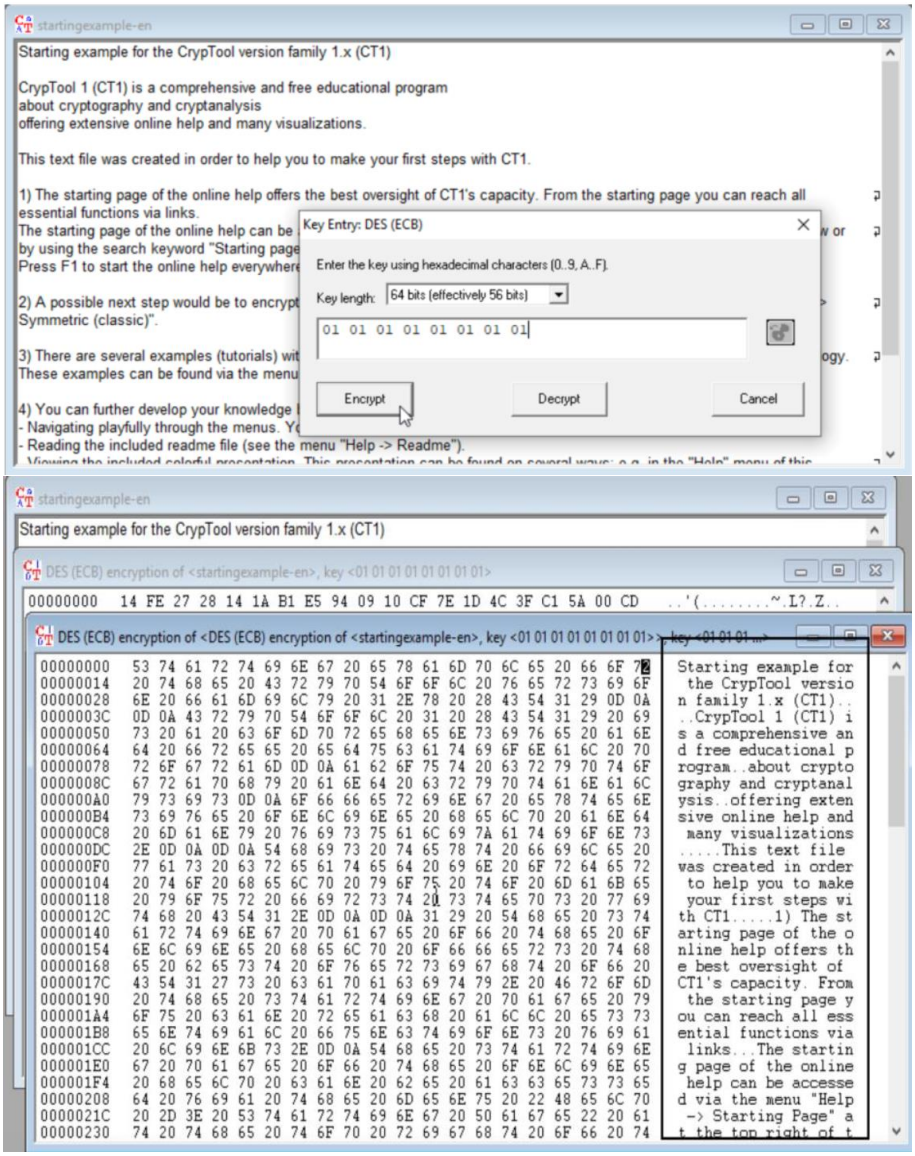
به همین ترتیب بقیه عناصر جدول نیز حاصل می شوند.

فصل سوم و چهارم

7.1

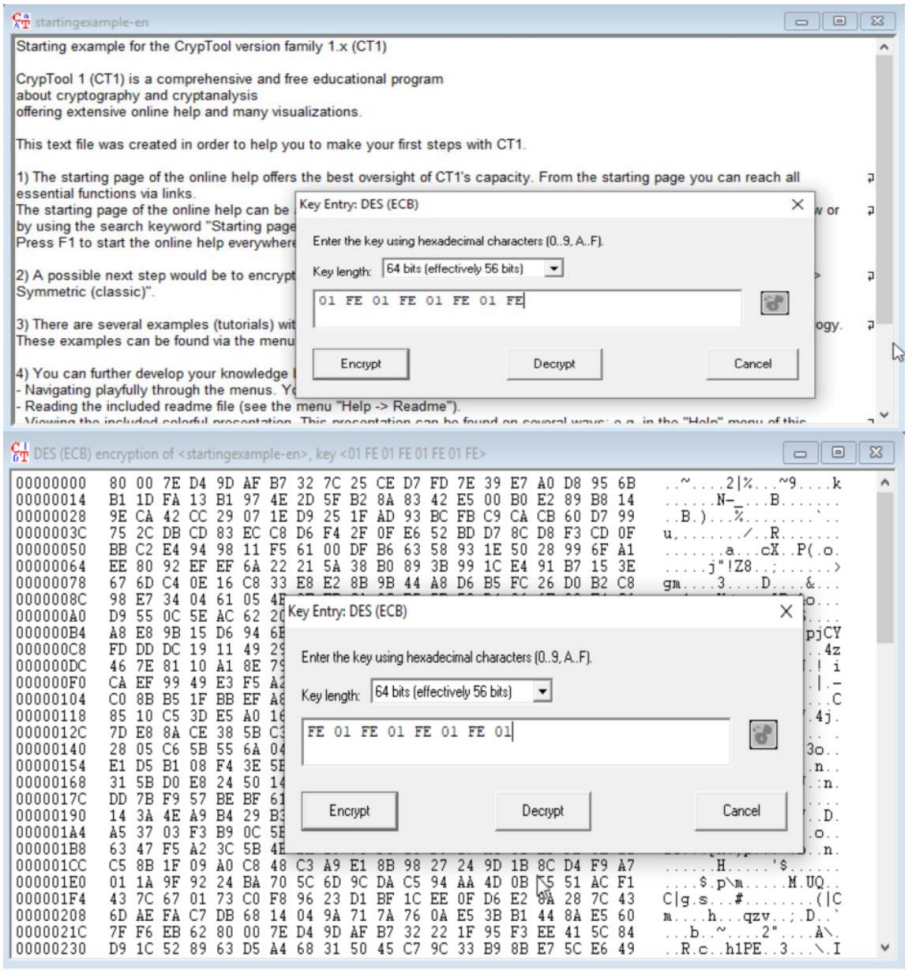


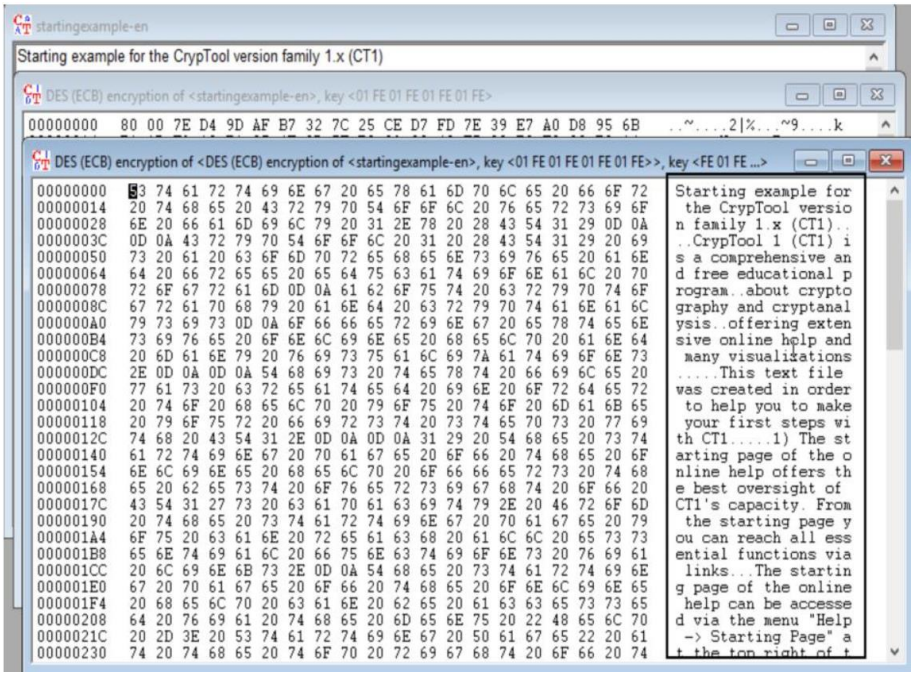
i.


startingexample-en
Starting example for the CrypTool version family 1.x (CT1)
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
by using the search keyword "Starting page
Press F1 to start the online help everywhere
2) A possible next step would be to encrypt
Symmetric (classic)".
3) There are several examples (tutorials) wit
These examples can be found via the menu
4) You can further develop your knowledge
- Navigating playfully through the menus. Y
- Reading the included readme file (see the menu "Help -> Readme").
Key Entry: DES (ECB)
Enter the key using hexadecimal characters (0..9, A..F).
Key length:
64 bits (effectively 56 bits)
01 01 01 01 01 01 01 01
Encrypt
Decrypt
Cancel

startingexample-en
Starting example for the CrypTool version family 1.x (CT1)
DES (ECB) encryption of <startingexample-en>, key <01 01 01 01 01 01 01 01>
00000000 14 FE 27 28 14 1A B1 E5 94 09 10 CF 7E 1D 4C 3F C1 5A 00 CD ..'(.....~.L?.Z..
DES (ECB) encryption of <DES (ECB) 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 20 65 78 61 6D 70 6C 65 20 66 6F 72 Starting example for
00000014 20 74 68 65 20 43 72 79 70 54 6F 6F 6C 20 76 65 72 73 69 6F the CrypTool versio
00000028 6E 20 66 61 6D 69 6C 79 20 31 2E 78 20 28 43 54 31 29 0D 0A n family 1.x (CT1)..
0000003C 0D 0A 43 72 79 70 54 6F 6F 6C 20 31 20 28 43 54 31 29 20 69 ..CrypTool 1 (CT1) i
00000050 73 20 61 20 63 6F 6D 70 72 65 68 65 6E 73 69 76 65 20 61 6E s a comprehensive an
00000064 64 20 66 72 65 65 20 65 64 75 63 61 74 69 6F 6E 61 6C 20 70 d free educational p
00000078 72 6F 67 72 61 6D 0D 0A 61 62 6F 75 74 20 63 72 79 70 74 6F rogram..about crypto
0000008C 67 72 61 70 68 79 20 61 6E 64 20 63 72 79 70 74 61 6E 61 6C graphy and cryptanal
000000A0 79 73 69 73 0D 0A 6F 66 66 65 72 69 6E 67 20 65 78 74 65 6E ysis..offering exten
000000B4 73 69 76 65 20 6F 6E 6C 69 6E 65 20 68 65 6C 70 20 61 6E 64 sive online help and
000000C8 20 6D 61 6E 79 20 76 69 73 75 61 6C 69 7A 61 74 69 6F 6E 73 many visualizations
000000DC 2E 0D 0A 0D 0A 54 68 69 73 20 74 65 78 74 20 66 69 6C 65 20 .....This text file
000000F0 77 61 73 20 63 72 65 61 74 65 64 20 69 6E 20 6F 72 64 65 72 was created in order
00000104 20 74 6F 20 68 65 6C 70 20 79 6F 75 20 74 6F 20 6D 61 6B 65 to help you to make
00000118 20 79 6F 75 72 20 66 69 72 73 74 20 73 74 65 70 73 20 77 69 your first steps wi
0000012C 74 68 20 43 54 31 2E 0D 0A 0D 0A 31 29 20 54 68 65 20 73 74 th CT1.....1) The st
00000140 61 72 74 69 6E 67 20 70 61 67 65 20 6F 66 20 74 68 65 20 6F arting page of the o
00000154 6E 6C 69 6E 65 20 68 65 6C 70 20 6F 66 66 65 72 73 20 74 68 nline help offers th
00000168 65 20 62 65 73 74 20 6F 76 65 72 73 69 67 68 74 20 6F 66 20 e best oversight of
0000017C 43 54 31 27 73 20 63 61 70 61 63 69 74 79 2E 20 46 72 6F 6D CT1's capacity. From
00000190 20 74 68 65 20 73 74 61 72 74 69 6E 67 20 70 61 67 65 20 79 the starting page y
000001A4 6F 75 20 63 61 6E 20 72 65 61 63 68 20 61 6C 6C 20 65 73 73 ou can reach all ess
000001B8 65 6E 74 69 61 6C 20 66 75 6E 63 74 69 6F 6E 73 20 76 69 61 ential functions via
000001CC 20 6C 69 6E 6B 73 2E 0D 0A 54 68 65 20 73 74 61 72 74 69 6E links...The startin
000001E0 67 20 70 61 67 65 20 6F 66 20 74 68 65 20 6F 6E 6C 69 6E 65 g page of the online
000001F4 20 68 65 6C 70 20 63 61 6E 20 62 65 20 61 63 63 65 73 73 65 help can be accesse
00000208 64 20 76 69 61 20 74 68 65 20 6D 65 6E 75 20 22 48 65 6C 70 d via the menu "Help
0000021C 20 2D 3E 20 53 74 61 72 74 69 6E 67 20 50 61 67 65 22 20 61 -> Starting Page" a
00000230 74 20 74 68 65 20 74 6F 70 20 72 69 67 68 74 20 6F 66 20 74 t the top right of t

ii.


startingexample-en
Starting example for the CrypTool version family 1.x (CT1)
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.
Key Entry: DES (ECB)
Enter the key using hexadecimal characters (0..9, A..F).
Key length: 64 bits (effectively 56 bits)
01 FE 01 FE 01 FE 01 FE
Encrypt
Decrypt
Cancel
DES (ECB) encryption of <startingexample-en>, key <01 FE 01 FE 01 FE 01 FE>
00000000 80 00 7E D4 9D AF B7 32 7C 25 CE D7 FD 7E 39 E7 A0 D8 95 6B
Key Entry: DES (ECB)
Enter the key using hexadecimal characters (0..9, A..F).
Key length: 64 bits (effectively 56 bits)
FE 01 FE 01 FE 01 FE 01
Encrypt
Decrypt
Cancel


startingexample-en
Starting example for the CrypTool version family 1.x (CT1)
DES (ECB) encryption of <startingexample-en>, key <01 FE 01 FE 01 FE 01 FE>
00000000 80 00 7E D4 9D AF B7 32 7C 25 CE D7 FD 7E 39 E7 A0 D8 95 6B
DES (ECB) encryption of <DES (ECB) encryption of <startingexample-en>, key <01 FE 01 FE 01 FE 01 FE>>, key <FE 01 FE ...>
00000000 53 74 61 72 74 69 6E 67 20 65 78 61 6D 70 6C 65 20 66 6F 72
Starting example for
the CrypTool versio
n family 1.x (CT1)..
..CrypTool 1 (CT1) i
s a comprehensive an
d free educational p
rogram..about crypto
graphy and cryptanal
ysis..offering exten
sive online help and
many visualizations
.....This text file
was created in order
to help you to make
your first steps wi
th CT1.....1) The st
arting page of the o
nline help offers th
e best oversight of
CT1's capacity. From
the starting page y
ou can reach all ess
ential functions via
links...The startin
g page of the online
help can be accesse
d via the menu "Help
-> Starting Page" a

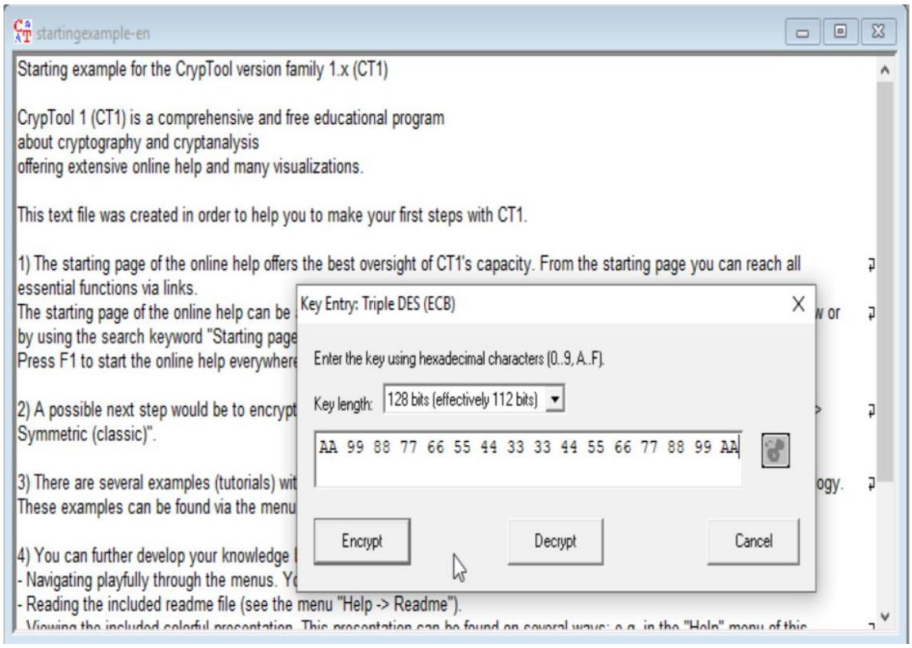
7.2.

i. Because its key space is larger.

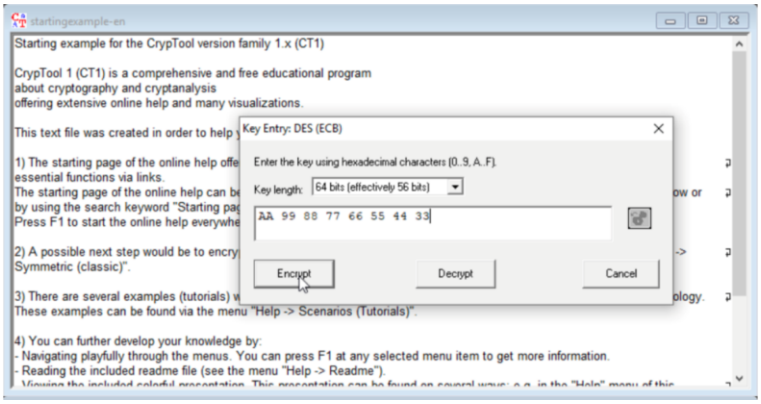
ii. key space = 2*56 = 112, that's because of meet in the middle attack.

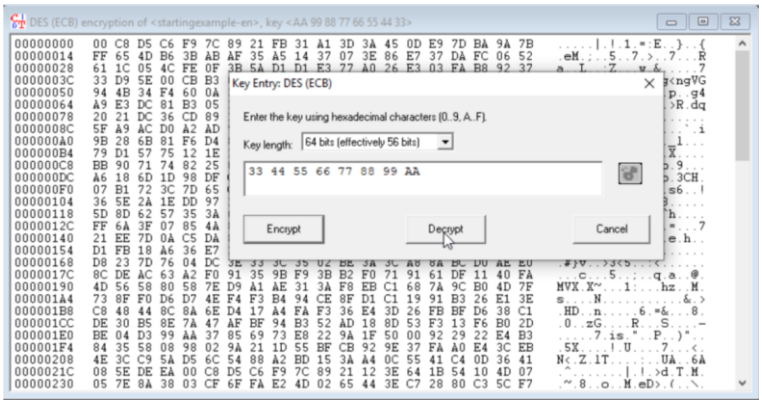
iii. Both versions are resistant to brute-force attacks as well as any analytical attack imaginable at the moment. However, the advantage of the second version over the first one is that 3DES performs single DES encryption if k3 = k2 = k1, which is sometimes desired in implementations that should also support single DES for legacy reasons.

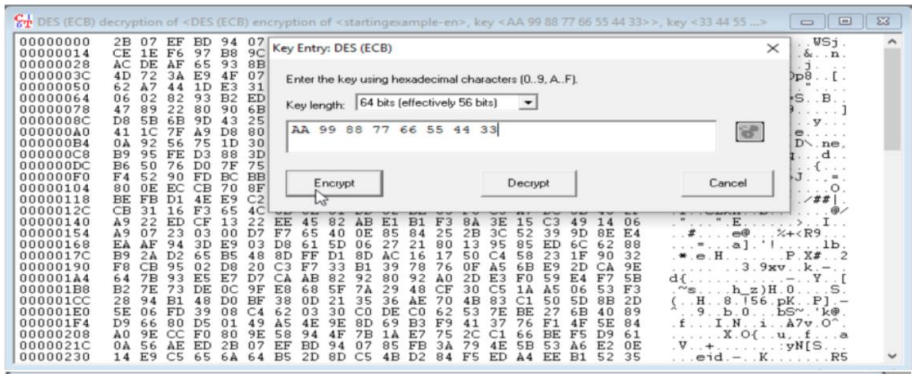
iv.



v.







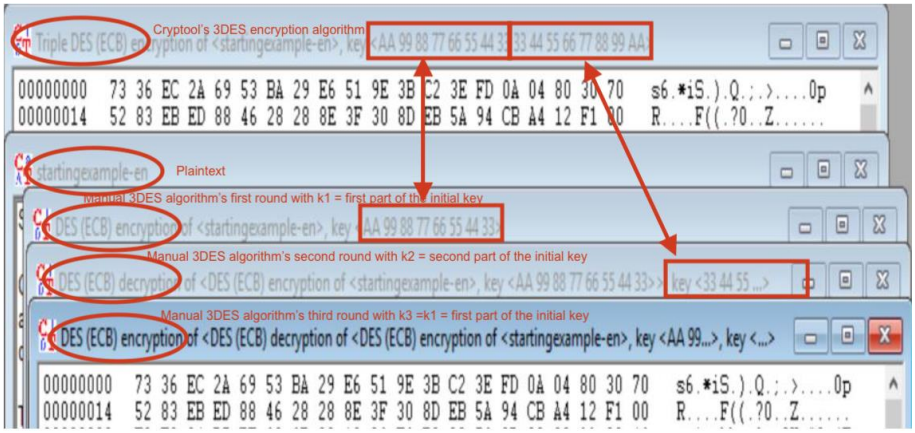
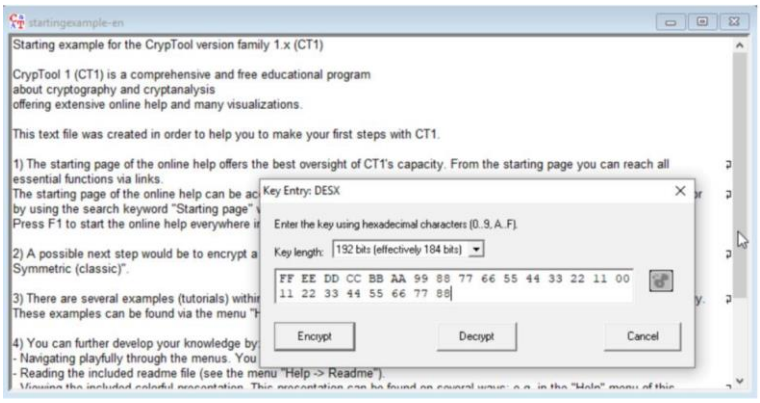


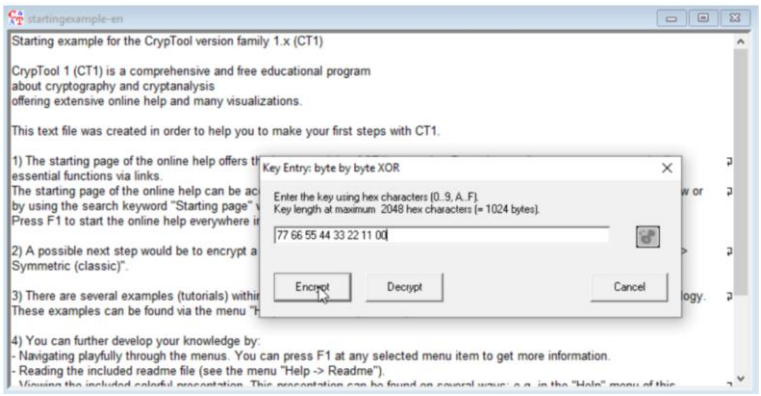
Figure: As observable in this figure, the output of Cryptool's 3DES algorithm is the same as our manually generated 3DES output.

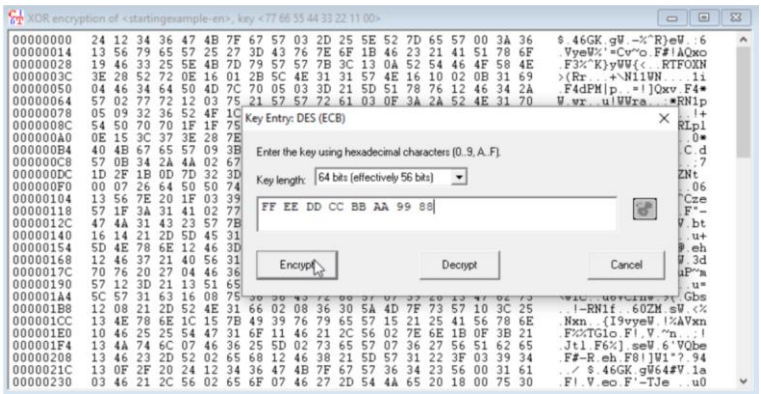
7.3.

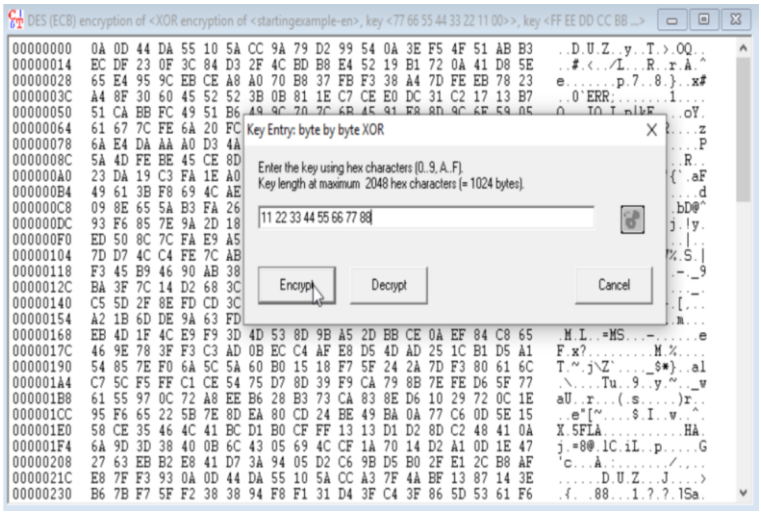
i.


startingexample-en
Starting example for the CrypTool version family 1.x (CT1)
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.
Key Entry: DESX
Enter the key using hexadecimal characters (0..9, A..F).
Key length: 192 bits (effectively 184 bits)
FF EE DD CC BB AA 99 88 77 66 55 44 33 22 11 00
11 22 33 44 55 66 77 88
Encrypt
Decrypt
Cancel
2) A possible next step would be to encrypt a
Symmetric (classic)".
3) There are several examples (tutorials) withir
These examples can be found via the menu "H
4) You can further develop your knowledge by
- Navigating playfully through the menus. You
- Reading the included readme file (see the menu "Help -> Readme").

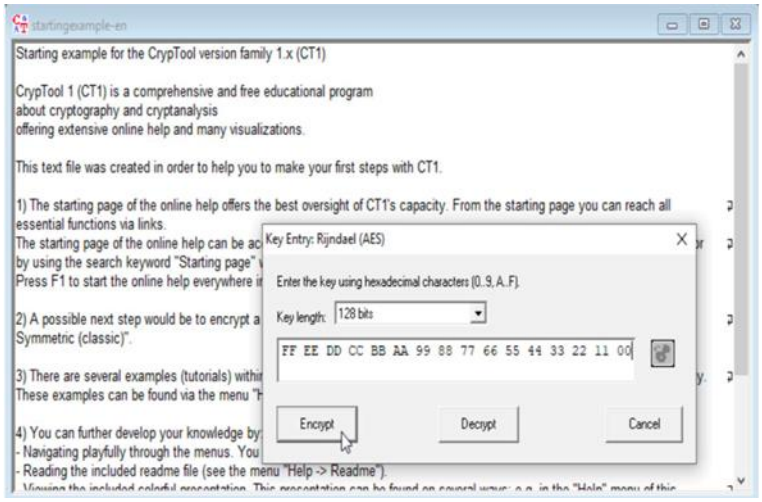
ii.


startingexample-en
Starting example for the CrypTool version family 1.x (CT1)
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.
Key Entry: byte by byte XOR
Enter the key using hex characters (0..9, A..F).
Key length at maximum 2048 hex characters (= 1024 bytes).
77 66 55 44 33 22 11 00
Encrypt
Decrypt
Cancel
2) A possible next step would be to encrypt a
Symmetric (classic)".
3) There are several examples (tutorials) withir
These examples can be found via the menu "H
4) You can further develop your knowledge by:
- Navigating playfully through the menus. You can press F1 at any selected menu item to get more information.
- Reading the included readme file (see the menu "Help -> Readme").


XOR encryption of <startingexample-en>, key <77 66 55 44 33 22 11 00>
Key Entry: DES (ECB)
Enter the key using hexadecimal characters (0..9, A..F).
Key length: 64 bits (effectively 56 bits)
FF EE DD CC BB AA 99 88
Encrypt
Decrypt
Cancel



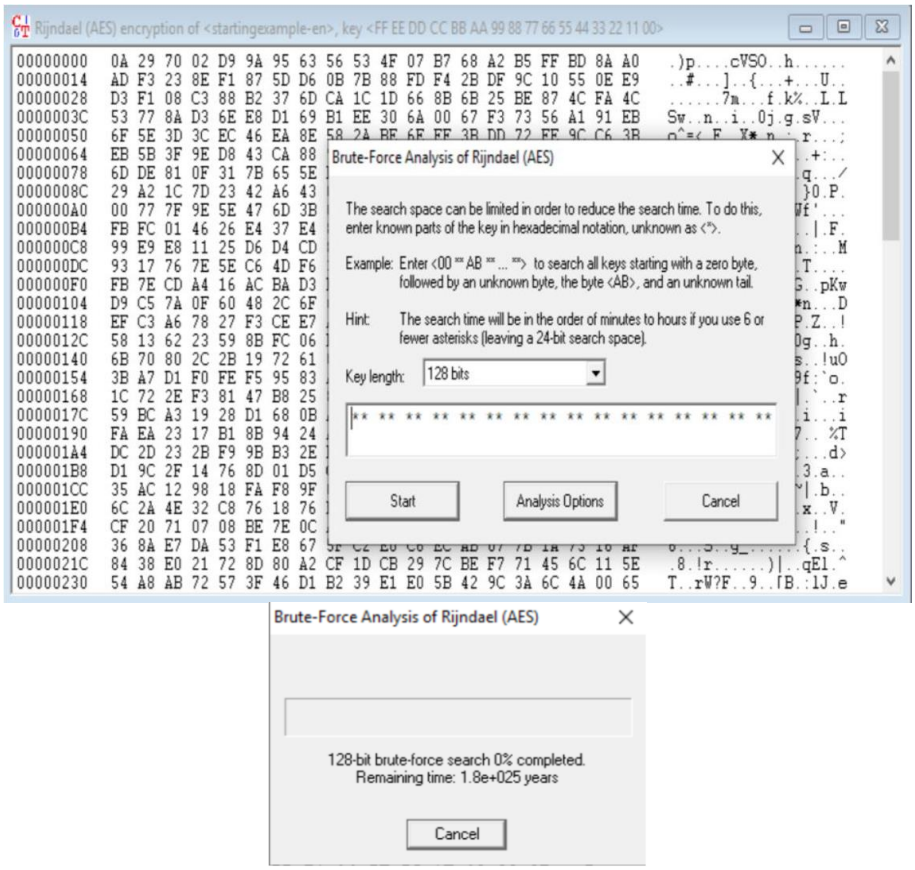
7.4.



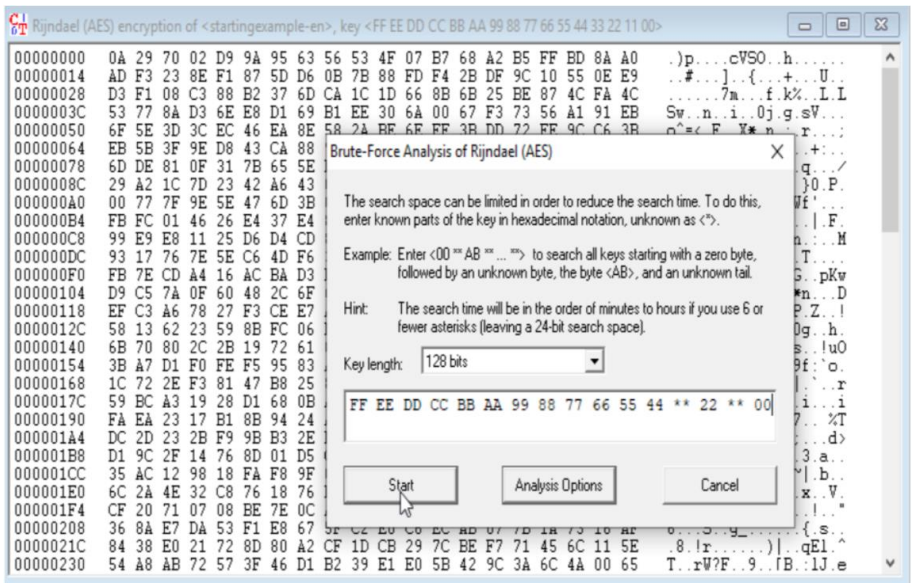
7.5.

i.

processing time = $(1.8*10^{25}*365*24*3600*10^{6})/2^{128}$ = 1.67 micro seconds.


Rijndael (AES) encryption of <startingexample-en>, key <FF EE DD CC BB AA 99 88 77 66 55 44 33 22 11 00>
Brute-Force Analysis of Rijndael (AES)
The search space can be limited in order to reduce the search time. To do this, enter known parts of the key in hexadecimal notation, unknown as <*>.
Example: Enter <00 ** AB ** ... **> to search all keys starting with a zero byte, followed by an unknown byte, the byte <AB>, and an unknown tail.
Hint: The search time will be in the order of minutes to hours if you use 6 or fewer asterisks (leaving a 24-bit search space).
Key length: 128 bits
** ** ** ** ** ** ** ** ** ** ** ** ** ** ** **
Start
Analysis Options
Cancel
Brute-Force Analysis of Rijndael (AES)
128-bit brute-force search 0% completed.
Remaining time: 1.8e+025 years
Cancel

ii.


Rijndael (AES) encryption of <startingexample-en>, key <FF EE DD CC BB AA 99 88 77 66 55 44 33 22 11 00>
Brute-Force Analysis of Rijndael (AES)
The search space can be limited in order to reduce the search time. To do this, enter known parts of the key in hexadecimal notation, unknown as <*>.
Example: Enter <00 ** AB ** ... **> to search all keys starting with a zero byte, followed by an unknown byte, the byte <AB>, and an unknown tail.
Hint: The search time will be in the order of minutes to hours if you use 6 or fewer asterisks (leaving a 24-bit search space).
Key length: 128 bits
FF EE DD CC BB AA 99 88 77 66 55 44 ** 22 ** 00
Start
Analysis Options
Cancel