

### ❖ مزیت های *OTP*

1. سادگی محاسباتی
2. عملیات رمزنگاری و رمزگشایی آن دارای *operation* های یکسانی است.
3. تا زمانی که در دنباله کلید تصادفی هر کلید به اندازه طول متن اصلی باشد دارای امنیت است.
4. صرفنظر از منابع محاسباتی مهاجم، احتمال متن ساده و متن رمز شده یکسان است.

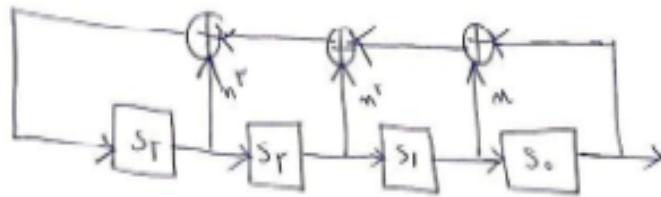
### ❖ مشکلات و معایب *OTP*

1. اندازه کلید باید به اندازه متن اصلی باشد.
2. ویژگی *Integrity* تضمین نمی شود.
3. در صورتیکه کلیدها مجددا استفاده شوند نامن بوده و مهاجم می تواند *XOR* متن اصلی را به دست آورد.
4. فقط *OTP* *Confidentiality* را تضمین می کند.
5. مهاجم متن اصلی را نمی تواند بازیابی کند ولی به راحتی می تواند متن اصلی را تغییر دهد.

به طور کلی سه نوع *LFSR* موجود است. تفاوت آن ها بدین شرح است:

1. *LFSR* هایی که یک دنباله واحد با طول حداکثر تولید می کنند این نوع *LFSR*ها به *LFSR*های مبتنی بر *primitive polynomials* معروف هستند.
2. *LFSR*هایی که دنباله با طول حداکثر تولید نمی کنند و طول دنباله مستقل از مقدار اولیه رجیستر(ثبات) می باشد. این نوع *LFSR*ها به *LFSR*های مبتنی بر *irreducible polynomials* معروف هستند.
3. *LFSR*هایی که یک دنباله با طول حداکثر تولید نمی کنند و طول آنها وابسته به مقدار اولیه رجیستر است این نوع *LFSR*ها به *LFSR*های مبتنی بر *reducible polynomials* معروف هستند.

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



با فرض مقدار اولیه دلخواه: 0001

مقدار اولیه	$S_3$	$S_2$	$S_1$	$S_0$	output
1	0	0	0	1	1
2	1	0	0	0	1
3	1	1	0	0	0
4	0	1	1	0	0
5	0	0	1	1	0
6	0	0	0	1	1

طول 5

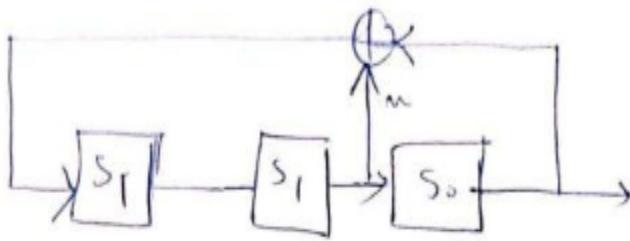
با فرض مقدار اولیه دلخواه: 1111

مقدار اولیه	$S_3$	$S_2$	$S_1$	$S_0$	output
1	1	1	1	1	0
2	0	1	1	1	1
3	1	0	1	1	1
4	1	1	0	1	1
5	1	1	1	0	1
6	1	1	1	1	0

طول 5

دیده می شود که ما در هر مورد یک دنباله مجزا با طول یکسان (5) داریم. طول دنباله مستقل از مقدار اولیه رجیستر ثبات) می باشد پس این چندجمله ای یک چندجمله ای از نوع irreducible است.

$$x^3 + x + 1$$



مقدار اولیه	$S_2$	$S_1$	$S_0$	output
1	0	0	1	1
2	1	0	0	0
3	0	1	0	1
4	1	0	1	1
5	1	1	0	1
6	1	1	1	0
7	0	1	1	0
8	0	0	1	1

طول 7

این نوع چندجمله ای از نوع primitive است. در اینجا یک دنباله با حداکثر طول حداکثر  $1 - 2^3$  داریم.

1-3- می دانیم که رمز مورد نظر یک رمز جریانی (stream cipher) است، پس با XOR کردن متن اصلی و متن رمز شده، کلید رمز بدست می آید:

$$\text{Plain text} \oplus \text{Cipher text} = \text{Key} = 0010111001011100101110010111$$

با توجه به کلید بدست آمده، در می باییم که کلید به صورت رشته بیت های 7 بیتی تکرار می شود، بنابراین دوره تناوب LFSR برابر با 7 بوده و درجه LFSR طبق رابطه  $2^m - 1 = 7$  برابر با 3 می شود.

$$\text{Key} = 0010111\ 0010111\ 0010111\ 0010111 \Rightarrow 2^m - 1 = 7 \Rightarrow m = 3$$

2-3- با توجه به این که درجه LFSR برابر با 3 است، بنابراین 3 بیت ابتدایی کلید با مقدار اولیه LFSR برابر است (3 بیت ابتدایی بدون تغییر از LFSR خارج می شوند).

$$\text{LFSR Initialization Vector} = 001 \Rightarrow s_0 = 0, s_1 = 0, s_2 = 1$$

3-3- با استفاده از ضرایب فیدبک LFSR، معادلات مربوط به 3 بیت بعدی ( $s_3$  تا  $s_5$ ) را تشکیل می‌دهیم: (توجه کنید که مقادیر این 3 بیت با استفاده از کلید مشخص است و فقط ضرایب فیدبک LFSR مجهول‌اند)

$$s_2 p_2 + s_1 p_1 + s_0 p_0 = s_3$$

$$s_3 p_2 + s_2 p_1 + s_1 p_0 = s_4$$

$$s_4 p_2 + s_3 p_1 + s_2 p_0 = s_5$$

اکون به کمک مقدار کلید (0010111)، ضرایب فیدبک را بدست می‌آوریم:

$$s_0 = 0, \quad s_1 = 0, \quad s_2 = 1 \quad \Rightarrow \quad 1p_2 + 0p_1 + 0p_0 = 0 \quad (s_3)$$

$$s_1 = 0, \quad s_2 = 1, \quad s_3 = 0 \quad \Rightarrow \quad 0p_2 + 1p_1 + 0p_0 = 1 \quad (s_4)$$

$$s_2 = 1, \quad s_3 = 0, \quad s_4 = 1 \quad \Rightarrow \quad 1p_2 + 0p_1 + 1p_0 = 1 \quad (s_5)$$

با حل 3 معادله و 3 مجهول بالا، ضرایب فیدبک به صورت زیر بدست می‌آیند:

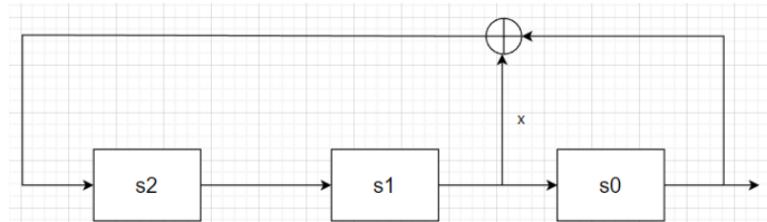
$$p_0 = 1, \quad p_1 = 1, \quad p_2 = 0$$

بنابراین چندجمله‌ای مربوط به LFSR به صورت زیر بدست می‌آید:

$$P(x) = x^3 + p_2 x^2 + p_1 x + p_0$$

$$\Rightarrow P(x) = x^3 + x + 1$$

4-3- بلوك دیاگرام LFSR مورد نظر به صورت زیر است:



با استفاده از بلوك دیاگرام LFSR و مقدار اوليه آن، خروجي را در هر دور محاسبه می‌کنیم:

$s_2$	$s_1$	$s_0$	خروچی
1	0	0	0 ( $s_0$ )
0	1	0	0 ( $s_1$ )
1	0	1	1 ( $s_2$ )
1	1	0	0 ( $s_3$ )
1	1	1	1 ( $s_4$ )
0	1	1	1 ( $s_5$ )

0	0	1	1 ( $s_6$ )
---	---	---	-------------

همان‌طور که مشاهده می‌شود، خروجی LFSR با کلید ما یکی است؛ بنابراین صحت نتایج بررسی می‌شود.

۴. در مرحله اول یا مرحله عبور از *initial permutation* اگر  $x$  متن اصلی باشد، به دلیل اینکه بیت 57 ام در متن اصلی ۱ است داریم:  $(x = 0000 \dots 010 \dots 0)$ .

$IP(x)$  بیت 57 را به بیت 33 نگاشت می‌دهد یعنی همه بیت‌ها صفر شده و فقط بیت ۳۳ می‌شود و وارد دور شماره یک می‌گردد. پس  $L_0 = 0 \dots 0 \dots 0 \dots 0000 \dots 010 \dots 0$  (32 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  $E(R_0)$ ، *expansion* بیت اول  $R_0$  را به بیت دوم و ۴۸ ام نگاشت می‌دهد. این یعنی مقادیر  $S_{2-7}$  در ورودی همه ۰ می‌گیرند.  $S_1$  در ورودی دارای مقدار  $010000_2$  است و  $S_8$  مقدار  $000001_2$  را می‌گیرد.

۲-۴. با عبور ورودی‌ها از  $s - box$  خروجی‌های زیر طبق جدول کتاب حاصل می‌شود.

	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 = 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  $R_1$  و  $L_1$  به شرح زیر است:

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

$$R_1 = D0585B9E_{16}$$

مینیمم تعداد بیت‌های خروجی ( $S - BOX$ ) که در نتیجه یک بیت تغییر در ورودی تغییر خواهد کرد برابر 2 است.

در حالتی که  $plaintext$  کاملاً صفر است با توجه به این که 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 بیت‌ها صفر باشند خروجی  $101100011011000110110110111100$  است و موردی که قبلاً محاسبه شده بود برابر  $1101000001011000010110110011110$  است. حاصل  $XOR$  نمودن این دو مقدار  $00001000100000001000000000100010$  است که نشان دهنده تغییر 5 بیت است به دلیل اینکه  $L_1$  مستقیماً وارد  $R_0$  شده و یک بیت از  $L_1$  نیز 1 است، مجموعاً دیده می‌شود به ازای تغییر 1 بیت در ورودی 6 بیت با هم تفاوت دارند.

$$\text{۵. به ازای هر } x \text{ داریم: } DES_k(x) = DES_k^{-1}(x)$$

در اینجا باید عمل رمزنگاری و رمزگشایی یکسان باشد. ترتیب کلیدهای مورد استفاده در رمزنگاری به صورت  $(k_1, k_2, k_3, \dots, k_{16})$  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:

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

.۲-۵

دارای 4 عدد *weak keys* از نوع 64 بیتی است. طبق نکته قسمت قبل برای اینکه شیفت بیت ها اثری نداشته باشد لذا داریم:

<i>Keys before parities drop (64 bits)</i>	<i>Actual key (56 bits)</i>
0101 0101 0101 0101	0000000 0000000
1F1F 1F1F 0E0E 0E0E	0000000 FFFFFFFF
E0E0 E0E0 F1F1 F1F1	FFFFFFF 0000000
FEFE FEFE FEFE FEFE	FFFFFFF FFFFFFFF

۳-۵. به طور کلی احتمال انتخاب یکی از این کلیدهای ضعیف به طور تصادفی برابر است با:

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

۴-۵. 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.

۵-۵. به طور کلی 6 زوج (جفت) یا 12 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

.۶-۵

دارای کلید *semi weak* است که تنها دو زیرکلید متفاوت تولید می کنند که هر کدام به تعداد 8 مرتبه در الگوریتم استفاده می شوند.

.۷-۵

دارای  $2^{56}$  کلید است. تعداد کل کلیدهای ممکن 64 عدد می باشد که 4 عدد *weak* ، 12 عدد *semi weak* و 48 عدد *possible weak key* 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:  $\frac{4+12+48}{2^{56}}$

.۶

.۱-۶

$$A \oplus B = (AB')V(A'B)$$

$$A' \oplus B' = ((A')(B')')V((A')'(B')) = (A'B)V(AB') = A \oplus B$$

$$\begin{aligned} A' \oplus B &= (A'B')V(AB) = (A'VA)(A'VB)(B'VA)(B'VB) = (A'VB)(B'VA) = \\ &((A'VB)' V (B'VA)')' = ((AB')V(A'B))' = (A \oplus B)' \end{aligned}$$

۲-۶. با توجه به این که تابع  $PC$  یک جایگشت مشخصی را بر روی بیت‌ها اعمال می‌کند، مکمل کردن (یا اصطلاحا flip کردن) بیت‌ها قبل یا بعد از آن تفاوتی به وجود نمی‌آورد؛ بنابراین  $' = (PC - 1(k)) = (PC - 1(k'))$  است.

۳-۶. مشابه با قسمت قبل، توابع چرخش زیر کلیدها نیز دارای جایگشت‌های مشخصی هستند و مکمل کردن (یا اصطلاحا flip کردن) بیت‌ها قبل یا بعد از آن تفاوتی ایجاد نمی‌کند، پس بنابراین  $' = (LS_i(C_{i-1})) = (LS_i(C_{i-1}'))$  است.

۴-۶. با توجه به این که  $2 - PC$  نیز مانند  $1 - PC$  یک جایگشت خطی است، همه‌ی عملیات‌ها برای تولید کلید خطی هستند؛ بنابراین اگر  $k'$  ورودی باشد، کلیدهای تولید شده  $i$  هستند.

۵-۶. مشابه با قسمت‌های قبلی،  $IP$  نیز خطی بوده و  $' = (IP(x))$  است.

۶-۶- تابع  $E$  که هر بیت در یک بردار را به یک یا دو بیت در یک بردار بزرگتر نگاشت یا اصطلاحا map می‌کند. با توجه به این که هیچ عملیات ترکیبی انجام نمی‌شود، هر بیت در بردار گسترش یافته حاصل از یک بیت در بردار اصلی است، پس مکمل کردن یک بیت قبل یا بعد از نگاشت کردن تفاوتی ایجاد نمی‌کند؛ بنابراین  $(E(R'_i)) = (E(R_i))$  است.

۷-۶- می‌دانیم که  $f(R_i, k) = P(S(E(R_i) \oplus k))$  است، بنابراین طبق نتایجی که تا کنون بدست آورده‌ایم، داریم:

$$f(R'_i, k') = P(S(E(R'_i) \oplus k')) = P(S(E(R_i)' \oplus k')) = P(S(E(R_i) \oplus k')) = f(R_i, k)$$

با توجه به این که  $R_i = L_{i-1} \oplus f(R_{i-1}, k)$  است، داریم:

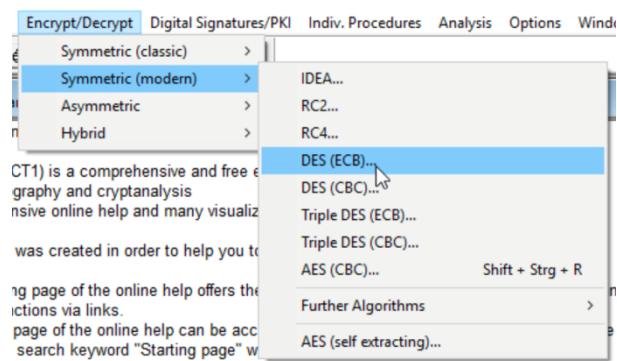
$$\Rightarrow L'_{i-1} \oplus f(R'_{i-1}, k') = L'_{i-1} \oplus f(R_{i-1}, k) = (L_{i-1} \oplus f(R_{i-1}, k))' = R'_i$$

۸-۶. با در نظر گرفتن نتایج قسمت ۷، در صورتی که بیتهای ورودی مکمل شوند، خروجی هر دور نیز مکمل می‌شود؛ بنابراین  $IP^{-1}(x') = (IP^{-1}(x))'$  خطی است، پس

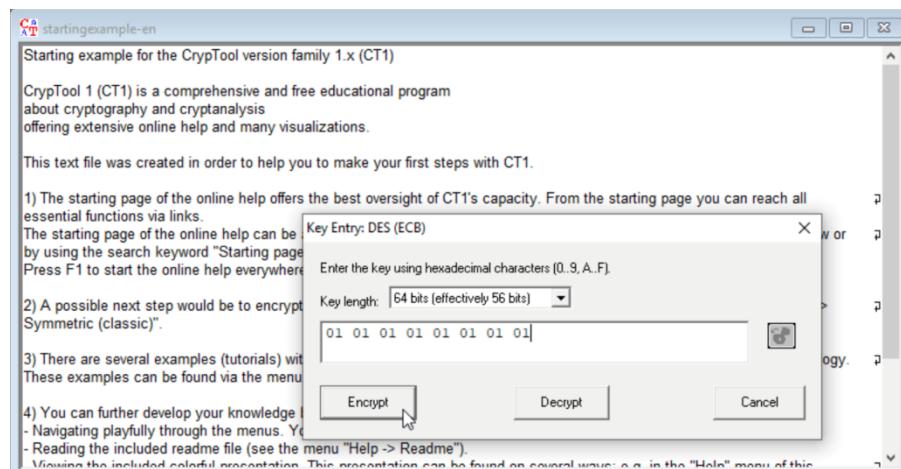
$$y = DES_k(x) \Rightarrow y' = DES_{k'}(x')$$

## ۷. تمرین کریپتو!

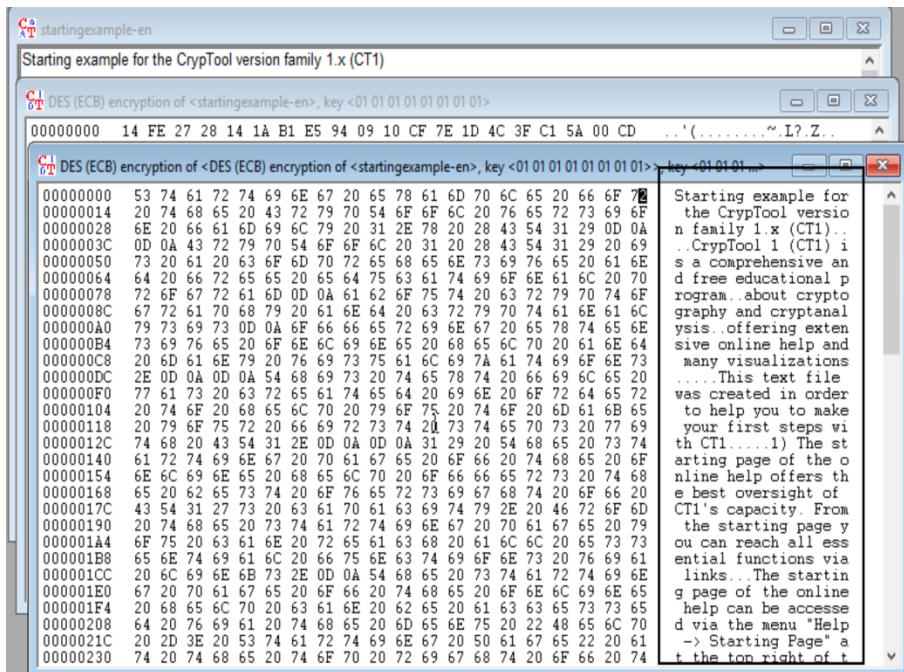
۷-۱



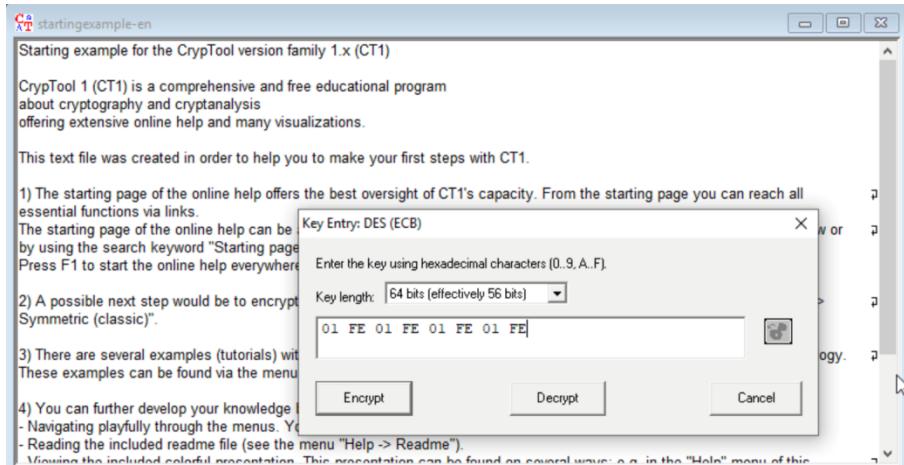
i)



## پاسخ تکلیف سری دوم مبانی رمزگاری



ii)



The top window is titled "CT DES (ECB) encryption of <startingexample-en>, key <01 FE 01 FE 01 FE 01 FE>". It displays a large block of hex data (00000000 to 00000230) and a "Key Entry: DES (ECB)" dialog box. The dialog box contains the key "FE 01 FE 01 FE 01 FE" and a "Key length: 64 bits (effectively 56 bits)" dropdown. Below the dialog are three buttons: "Encrypt", "Decrypt", and "Cancel".

The bottom window is titled "startingexample-en" and "Starting example for the CryptTool version family 1.x (CT1)". It also displays the same hex data and includes a large text area on the right side containing the following text:

```

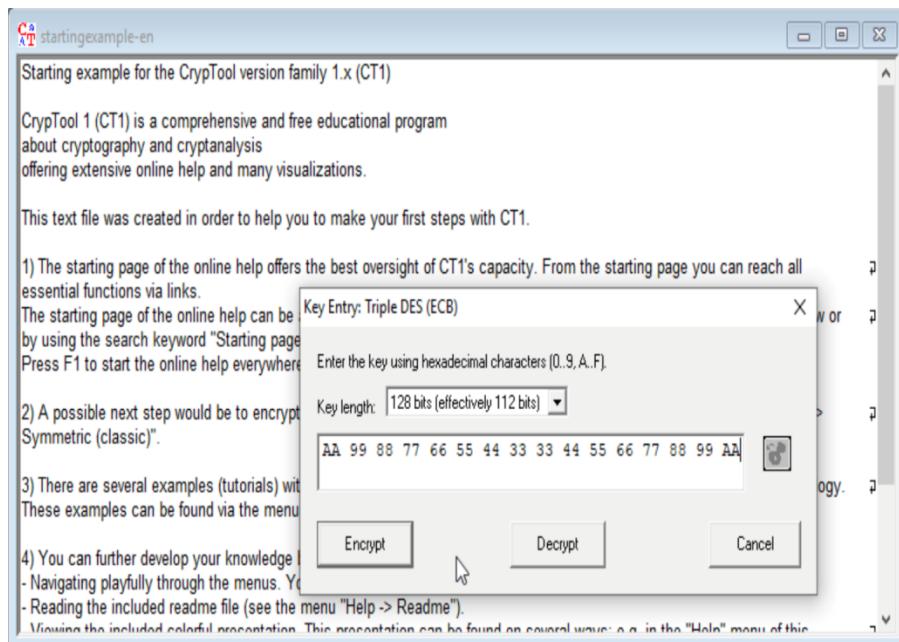
Starting example for
the CryptTool versio
n family 1.x (CT1)
..CryptTool 1 (CT1) i
s a comprehensive an
d free educational p
rogram..about crypto
graphy and cryptanal
ysis..offering exten
sive online help and
many visualizations
....This text file
was created in order
to help you to make
your first steps 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 accessse
d via the menu "Help
-> Starting Page" a
t the top right of t

```

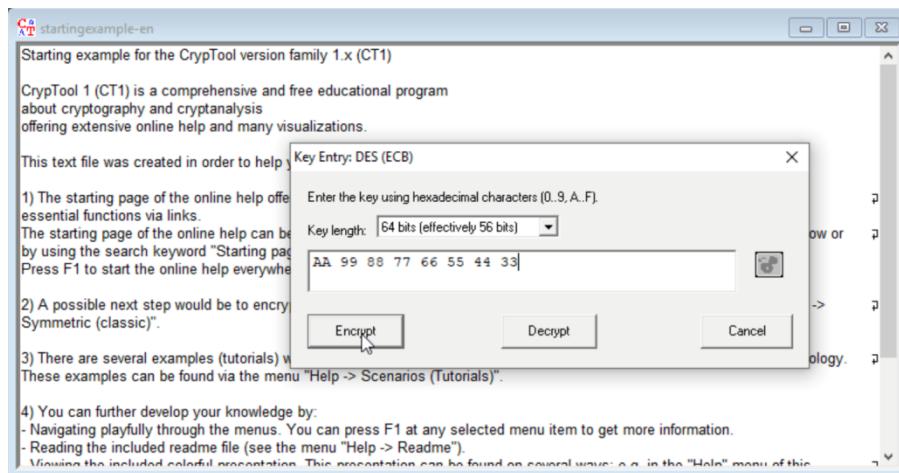
۷-۲

- 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  $k_3 = k_2 = k_1$ , which is sometimes desired in implementations that should also support single DES for legacy reasons.

iv)



v)



## پاسخ تکلیف سری دوم مبانی رمزنگاری

**CT DES (ECB) encryption of <startingexample-en>, key <AA 99 88 77 66 55 44 33>**

00000000	00 C8 D5 C6 F9 7C 89 21 FB 31 A1 3D 3A 45 0D E9 7D BA 9A 7B	... . ! . 1 . = . E . } . {
00000014	FF 65 4D B6 3B AB A5 14 37 07 3E 86 E7 37 DA FC 06 52	eM ; . 5 . 7 . > . 7 . . R
00000028	61 1C 05 4C FB 0F 3B 5A D1 D1 E3 77 A0 26 E3 03 FA BB 92 37	a L : Z w & . 7
0000003C	33 D9 5E 00 CB B3	Key Enter: DES (ECB)
00000050	94 4B 34 F4 60 0A	x gngVG
00000064	A9 E3 DC 81 B3 05	p . g4
00000078	20 21 DC 36 CD 89	>R.dq
0000008C	9F A9 A6 D0 A2 AD	: i
000000A0	98 2B 6B 81 F6 D4	X . . .
000000B4	79 D1 57 75 12 F6	p . 9
000000C8	BB 90 71 74 82 25	p . 3CH
000000DC	A6 18 6D 1D 98 DF	s6 . !
000000F0	07 B1 72 3C 7D 65	s . .
00000104	36 5E 2A 1E DD 97	h . .
00000118	5D 8D 62 57 35 3A	= . 7
0000012C	FF 6A 3F 07 85 4A	e . h .
00000140	21 EE 7D 0A C5 DA	
00000154	D1 FB 18 A6 36 E7	
00000168	D8 23 7D 76 04 DC	. # } v . . > 3 < S . .
0000017C	8C DE AC 63 A2 F0	. c . 5 . ; q . a . @
00000190	4D 56 58 80 58 7E	MVX . X ~ . . 1 . . h z . M
000001A4	D9 A1 AE 31 3A F8	C . N . . & . >
000001B8	EB C1 68 7A 9C B0 4D	HD . n . . . 6 . = & . . 8 .
000001CC	73 88 F6 D7 4B F4	0 . zG . . R . S . -
000001E0	B3 F3 B4 94 CE 8F	. 7 is . " P . ) " .
000001F4	D1 C1 19 91 B3 26	5X . ! U . . 7 . . < .
00000208	E1 29 8E 8A 6B 4F	N < Z . IT . . . U A . 6A
0000021C	5D C6 F9 7C 89 21	.   . > d . T . M .
00000230	12 3E 64 1B 54 10 D0	. ~ . 8 . o . M . eD . ( . \ .

**CT DES (ECB) decryption of <DES (ECB) encryption of <startingexample-en>, key <AA 99 88 77 66 55 44 33>, key <33 44 55 ...>**

00000000	2B 07 EF BD 94 07	VSj .
00000014	CE 1E F6 97 B8 9C	& . n .
00000028	AC DE AF 65 93 8B	j .
0000003C	4D 72 3A E9 4F 07	Dp8 . [
00000050	62 A7 44 1D E3 31	-S . B . ]
00000064	0A 92 58 80 58 7E	y . .
00000078	47 89 22 80 90 6B	D . ne .
0000008C	D8 5B 6B 9D 43 25	t . d .
000000A0	41 1C 7F A9 D8 80	J . = .
000000B4	D9 92 58 80 1B 30	# . O .
000000C8	B9 92 58 80 1B 30	
000000DC	B6 50 76 D0 7F 75	
000000F0	F4 52 95 FD BC BB	
00000104	80 0E ED CB 70 0F	
00000118	BE FB D1 4B E9 C2	
00000132	C0 92 58 80 1B 30	
00000140	A9 22 ED CF 13 22 EE 45	" . . . E . > . i . /
00000154	A9 07 20 03 00 D7 F7	# . . a! . ! . 1b .
00000168	65 40 0E 85 84 25 2B	ED 6C 62 88 . . . .
00000182	3D E9 03 D8 61 ED 06	27 21 80 13 95 85
00000196	2D E9 03 D8 61 ED 06	A1 17 5A 26 95 85
000001A0	2D E9 03 D8 61 ED 06	2D 00 32 95 85
000001A4	2D E9 03 D8 61 ED 06	F5 A5 6B E9 2D 00 32
000001B8	64 7B 93 E5 E7 D7 CA	AB E8 92 80 92 A0 2D E3 F0 59 E4 F7 SB
000001CC	BF 38 OD 21 35 36 AE	70 4B 83 C1 50 5D 8B 2D
000001E0	70 4B 83 C1 50 5D 8B	2D 40 40 89
000001F4	2D 40 40 89	
00000208	A0 9E CC ED 04 80 9E	58 94 4F 7B 1E 75 2C C1 66 BE F5 D9 61
0000021C	52 83 EB ED 88 46 28 28	E3 F0 59 4B 3A 79 4E 5B 53 A6 E2 0E
00000230	8E 3F 30 8D EB 5A 94	CB A4 12 F1 00

**CT Triple DES (ECB) encryption of <startingexample-en>, key <AA 99 88 77 66 55 44 33 33 44 55 66 77 88 99 AA>**

00000000	73 36 EC 2A 69 53 BA 29 E6 51 9E 3B C2 3E FD 0A 04 80 30 70	s6 . * iS . ) . Q . ; . > . . 0p
00000014	52 83 EB ED 88 46 28 28 8E 3F 30 8D EB 5A 94 CB A4 12 F1 00	R . . . F( ( . ? 0 . Z . . . .

vi)

## پاسخ تکلیف سری دوم مبانی رمزگاری

**CrypTool DES (ECB) encryption of <DES (ECB) decryption of <DES (ECB) encryption of <startingexample-en>, key <AA 99...>, key <...>**

00000000	73 36 EC 2A 69 53 BA 29 E6 51 9E 3B C2 3F FD 0A 04 80 30 70	s6.*iS.) Q.:>...Op
00000014	52 83 EB ED 88 46 28 8E 3F 30 8D EB 5A 94 CB A4 12 F1 00	R...F((?0:Z...Op
00000028	F2 F0 24 D7 BE 68 6B 98 12 26 E6 B9 38 55 9D 22 32 AA 28 46	\$..hk...&..8V"2(F
0000003C	29 80 86 2E BD 89 68 41 DF 90 02 AD B9 85 0A 51 5B D7 82 51	)....hA....Q[...Q
00000050	84 DA 85 E5 76 4C 04 C1 80 F0 83 9D 04 AE F2 F9 6E 2A 85 26	.vL...n*...w.t.C.=... <H...v9Y
00000064	E0 77 07 74 D8 43 15 3D 8C 8E 7C 3C 1D 48 8A 12 9A 76 39 59	.U...P...~(9...y^
00000078	D8 0E 55 BE 80 00 DE 81 19 50 2E 02 E4 F6 28 39 20 D6 79 7E	.G.p...~S...o#...1
0000008C	BB A4 84 47 E0 70 C7 7B AD 24 0D EF BB D0 6F 23 D7 5D 0A F1	.2.u...F .%G.Y
000000A0	DA BF 2E CF BB 8E DC 32 7F 75 C6 D6 46 7C E7 25 47 03 59 A4	
000000B4	AF C4 AD 8A 72 26 7E	
000000C8	3C 34 5C C1 93 15 44	
000000DC	6A 0D 23 3C AA 05 E1	
000000F0	E8 7D 0B 3F 91 D2 A6	
00000104	4B 2C 2B D5 D3 5D 95	
00000118	2D B3 6A 00 36 35 CE	
0000012C	62 EB E4 42 F7 E3 EC	
00000140	CC 5B 10 0A 88 0F 2E	
00000154	17 DE 10 D6 2B 79 42	
00000168	FB 8D 41 8B 6B 84 67	
0000017C	80 07 7D 1B 4F 54 BF	
00000190	FE 41 04 99 38 C2 91	
000001A4	53 B0 FD F8 C4 76 88	
000001B8	9C 15 2B 6F 81 F4 D0	
000001CC	70 01 B6 99 3B DA 53	
000001E0	77 D1 1C 6C 4F 7E 14	
000001F4	16 31 AD 2A 8A 7A FA 9C A1 45 63 C9 D0 02 5A 08 B8 BD 21 5E	.1.*.z...Ec...Z...!
00000208	C7 BB 9D 06 E0 1B 77 9E 95 B4 00 1B 95 AA E4 51 60 C5 CD B4	.1...v...Q...a.s6*iS)...)
0000021C	1A 8A 61 D5 73 36 EC 2A 69 53 BA 29 F6 16 80 B1 B8 A6 8F DF	1...Pz...u}SH.b.c1
00000230	5D B7 F5 81 50 7A BB 8E 80 75 7D 53 48 0D D9 62 A4 C9 63 31	

**Key Entry: Triple DES (ECB)**

Enter the key using hexadecimal characters (0..9, A..F).

Key length: 128 bits (effectively 112 bits)

AA 99 88 77 66 55 44 33 33 44 55 66 77 88 99 AA
---

Encrypt Decrypt Cancel

**CrypTool DES (ECB) encryption of <DES (ECB) decryption of <DES (ECB) encryption of <startingexample-en>, key <AA 99...>, key <...>**

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 60 20 68 65 60 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
000000D2	2E 0D 0A 0D 0A 54 68 69 73 20 74 65 78 74 20 66 69 6C 65 20	.....This text file
000000E0	77 61 73 20 63 72 63 61 74 65 64 20 69 6E 20 67 72 64 65 72	was created in order
00000104	20 74 6F 20 68 65 66 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	68 6C 69 6E 65 20 68 65 60 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 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 20 65 73 73	ou can reach all es
000001B8	65 6E 74 69 61 6C 20 66 75 6E 63 74 69 6F 6E 73 20 76 69 61	sential functions via
000001C2	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
00000208	20 68 65 6C 70 20 63 61 6E 20 62 65 20 61 63 63 65 73 73 65	help can be accessed
0000021C	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
00000230	20 2D 3E 20 53 74 61 72 74 69 6E 67 20 50 61 67 65 22 20 61	-> Starting Page" a

