Assignment 5

Task 1: Lab on Testing Different Modes in Symmetric Ciphers



Symmetric key cryptography provides several modes of operation, including Electronic Codebook (ECB), Cipher-Block Chaining (CBC), Cipher Feedback (CFB), Output Feedback (OFB), and Counter Mode (CTR), as shown in Figure 1. Modes of operation have been devised to encipher text of any size employing either DES or AES. Two important properties of these encryption modes that this lab will explore are **pattern preservation** and **error propagation**. Pattern preservation means that a block of plaintext is encrypted into a block of cipher text the same way every time; e.g. if Eve finds out that cipher text blocks 1, 5, and 10 are the same, she knows that plaintext blocks 1, 5, and 10 are the same. Error propagation means that a single bit error in transmission of a cipher text block creates errors in not only the decryption of the affected block, but propagates to the following blocks of the message.



Figure 1. Modes of Operation

Lab Tasks

Create an application to encrypt and decrypt messages using DES or AES ciphers using a programming language/cryptographic package of your own choice. Java has a mature offering in the form of its Java Cryptography Extension, which is integrated with the Java 2 SE SDK. An article on using AES with Java can be found here:

<u>http://java.sun.com/developer/technicalArticles/Security/AES/AES_v1.html</u>. BSAFE from RSA is available under share project. You can choose a language/package that allows for the selection of operation mode (ECB, CBC, etc.) for encryption/decryption.

Task 1 Implement DES and AES ciphers. (50 points)

Create an application in the language of your choice that implements encryption of a plaintext series of bytes, and decryption of the created cipher text.

Task 2 Investigate Properties of Modes in DES and AES (50 points)

Your application should use either AES or DES encryption, and employ each of the following algorithm modes: ECB, CBC, CFB, OFB, and CTR. Your application should test pattern preservation by encrypting plaintext that includes a pattern, and examining the cipher text to see if the pattern is preserved. Your program should test error propagation by modifying one byte of the cipher text prior to decryption, and then examining the decrypted plaintext. The output from your program should resemble the following:

opmode: CFB

input : 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 00 01 02 03 04 05 06 07

cipher: 61 a1 f8 86 ff 9b c7 09 4f c0 bc 1b 17 3a d7 bb c7 d7 1a 36 61 45 dd a8

Modifying random byte: bb->ba

plain : 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e <mark>0e 34 8b 0c bf fb 7f 9c de</mark>

Prepare a written report of your examination of the two discussed properties of the different cryptographic modes of operation. Include a completed version of the table below in your report (fill in each block with a yes, no, or other comment). Include the source code of your application with your report.

	ECB	СВС	CFB	OFB	CTR
Pattern preservation					
Error propagation					

Hint:

To test pattern preservation property, you can include repeated blocks in your plaintext and observe the results of cipher text.

To test error propagation property, you can encrypt plaintext first and then modify one bit in ciphertext and check the decryption results.

Taks 3: Triple DES with CBC mode and Weak DES keys (practice)

1. Open file "CrypTool-en.txt" from "C:\Program Files (x86)\CrypTool\examples".

2. Look at the frequency distribution of the characters by clicking "Analysis\Tools for Analysis \ Histogram".



3. Encrypt the document by selecting "Encrypt/Decrpt\Symmetric (modern)\Triple DES (CBC)".



4. Use **12 34 AB CD** as the key.

Key Entry: Triple DES (CBC)				
Enter the key using hexadecimal characters (09, AF). Key length: 128 bits (effectively 112 bits) 💌				
12 34 AB CD 00 00 00	00 00 00 00 00 00	00 00 00		
Encrypt	Decrypt	Cancel		

5. Click the **Encrypt** button.

😭 CrypTool 1.4.30 - Triple DES (CBC) encryption of <cryptool-en.txt>, key <12 34 AB CD 00 00 00 00 00 00 00 00 00 00 00 00 00</cryptool-en.txt>				
Elle Edit View Engrypt/Decrypt DigitalSignatures/PKI Indiv. Procedures Analysis Options Window Help				
AT cipitorenai				
What is Cryption?				
CrypTool is a freeware program which enables you to apply and analyse				
CrypTogla C, Triple DES (CBC) encryption of <cryptogl-en.txt>, key <12 34 AB CD 00 00 00 00 00 00 00 00 00 00 00 00 00</cryptogl-en.txt>				
orthour at a orthour at a<	$ \begin{array}{cccccccccccccccccccccccccccccccccccc$			

6. Look at histogram of the encrypted document, which bears no resemblance to the histogram of the unencrypted document.





7. The autocorrelation exhibits no regularity which may provide a clue as to the key length.

8. The decryption of the document functions like encryption except that the Decrypt button is clicked.

9. We want to determine the key from the encrypted document using a brute-force attack.

Select "Analysis\Symmetric Encryption (modern)\Triple DES (CBC)" from menu. Enter ** ** AB CD 00 00 00 00 00 00 00 00 00 00 as the key.

Brute-Force Analysis of Triple DES (CBC)			
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.</ab>			
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 (effectively 112 bits) 💌			
** ** AB CD 00 00 00 00 00 00 00 00 00 00 00 00 00			
<u>Start</u> <u>Analysis Options</u> <u>C</u> ancel			

10. Click "Start".

Brute-Force Analysis - Results

After a brute-force analysis of the given ciphertext decrypted with all possible keys in the selected key space, the entropy value of each decryption was calculated. This list contains the decrypted messages with the lowest entropy values. It is possible that the decryption with the smallest entropy is not the correct decryption, especially for very short ciphertexts. You can choose here which candidate you believe to be the correct decryption (note that only the first 128 characters are decrypted and displayed).

х

Entropy	Decryption: hex dump	Decryption	Key	*
4.2241	57 68 61 74 20 69 73 20 43 72 79 7	What is CrypTool?CrypTool is a fr	1234ABCD0000000000	
5.8924	B0 25 4C 9E 6F 36 D4 3B 6E 36 3C 1	.%L.o6.;n6 <i.fa.5e:};9co.a< td=""><td>C2AAABCD0000000000</td><td>=</td></i.fa.5e:};9co.a<>	C2AAABCD0000000000	=
5.9059	DA 69 BE E1 C5 8F C9 46 10 A1 D9	.iFO.~3.a^O`I.A	E068ABCD0000000000	
5.9111	4A 58 F7 44 A9 E4 AA 53 99 01 95 A	JX.DST:3rSy.'YYKM	2418ABCD000000000	
5.9177	D4 C9 F1 41 4E CF DC 56 28 D6 98	ANV(1.D.z.VHu!J.Uez8	DE04ABCD0000000000	
5.9313	5E 1B 38 CF 74 6D 73 D5 48 38 B4 1	^.8.tms.H8gSo0.wZ*>.&	02D0ABCD0000000000	
5.9326	D5 96 3E 8F EE 7B 05 83 E9 25 E4 A	>{%mC9z.aOc.O	BE9AABCD0000000000	
5.9326	8E 32 B1 57 5C AB 8C 96 EE 66 96 8	.2.W\f?.{W\Ie'\.!!	4A04ABCD0000000000	
5.9334	81 D8 96 77 76 83 DE 6F 96 3C 76 C	wvo. <vs]dm.i.ko0ii<< td=""><td>5292ABCD000000000</td><td></td></vs]dm.i.ko0ii<<>	5292ABCD000000000	
5.9385	FC 1B F7 D5 C6 2F 54 71 3B EF 80 E	/Tq;HIOO	F866ABCD000000000	
5.9431	D2 2C 20 FD 65 AD B2 F2 A1 4F AC	., .eOaTh)Z*fG.8	6A1AABCD0000000000	
5.9469	BE 45 1A 21 0B 8B C9 4F 1A 4B 3A 0	.E.!O.K:W0SEx.W	6A10ABCD0000000000	
5.9482	97 41 1C 9C AA 0C F2 A1 2B AC F0	.A+Md!p."KZ+	12CCABCD000000000	-
1.5.0400		to to the met	COEC + D CD AAAAAAAAAAAAA	
			t selection <u>C</u> ancel	

11. The first one returns readable results. Click "Accept selection". The original plaintext shows up.

CrypTool 1.4.30 - Triple DES (CBC) Analysis of <triple (cbc)="" <cryptool-en.txt="" des="" encryption="" of="">, key <12 34 AB CD 00 00 00 00 00 00 00 00 00 00 00 00 00</triple>			
The File View Encount/Decout Distal Sinasture/PKL Indix Procedures Analysis Ontions Window Help			
DIRIGIDIA			
Strate CrypTool-en.t			
W	10		
St Triple DES	(CBC) encryption of <cryptool-en.txt>, key <12.34 AB CD 00 00 00 00 00 00 00 00 00 00 00 00 00</cryptool-en.txt>		
00000000			
C 0000004E	Ym Triple DES (CBC) Analysis of <triple (cbc)="" <cryptool-en.txt="" des="" encryption="" of="">, key <12 34 AB CD 00 00 00 00 00 00 00 00 00 00 00 00 00</triple>		
W 00000075	What is CrypTool?		
000000C3	CryoTool is a freeware program which enables you to apply and analyse		
fu 000000EA	cryptographic mechanisms.		
00000138	CrypTool contains an exhaustive online help, which can be understood		
T 00000186	without deep knowledge in cryptography, therefore no user manual on now to use Constrol is provided Crysten is completely wailable in Fenish		
e 000001AD	and German CrypTool has implemented almost all state-of-the-art crypto		
a 000001FB	functions and allows you to learn about and use, modern and classic		
A 00000222	cryptography.		
^{III} 00000270	The methods available include both classic methods (e.g. the Caesar		
A 00000297	encryption algorithm) and modern cryptosystems (for example, the RSA		
k 000002E5	and AES algorithms, as well as algorithms based on elliptic curves).		
00000333	A summary of all the encryption algorithmsverschlverfahren available		
0000035A	in cryproor is contained on the help page for the crypt menu.		
c 000003A8	Automatic analysis tools for obtaining the key, starting from a		
T 000003CF	knowledge of the encrypted document and any additional information		
0000041D	(the unencrypted document or language of the document), are provided for the classic association alread/theraol information on		
00000444	automatic classic encyption agontamis. For adoutonal minimation of the automatic analysis, or to the help screen for the Analysis menu and		
00000492	choose the encryption algorithm to be analysed there.		
000004E9	To support your own analysis of documents, CrypTool can display a		
00000507	Instogram of the document, calculate the statistics for any re-grams and the entropy and auto-provelation		
00000555	no entropy and addedictedutor.		
0000057C			

Weak DES Keys

1. Click Encrypt/Decrypt\Symmetric(modern)\DES(ECB) when CrypTool-en.txt is open. Enter 01 01 01 01 01 01 01 01 as the key.

Key Entry: DES (ECB)			
Enter the key using hexadecimal characters (09, AF). Key length: 64 bits (effectively 56 bits)			
01 01 01 01 01 01 01	6		
<u>Encrypt</u>	Decrypt	Cancel	

2. Click "Encrypt" button.

File Edit View Encrypt/Decrypt DigitalSignatures/PKI Indiv. Procedures Analysis Options Window Help				
Str Str DES (EC) Wha 0000000 0000000 Cryp 0000000 0000004 Cryp 00000004 00000004) encyption of <cyptool-en.btr, <01010010101010101010<br="" key="">BE D0 3D ED 3E 25 55 1D D1 33 DF 0D 5C 2C 94 21 D9 F4 03 AB 42 55 83 F7 45 CE B5 EB 3E 33 21 A5 B8 09 22 23 09 1B 51 57 B9 34 EF C3 25 C4 C5 85 98 55 38 69 9C 52 49 7E 09 55 48 B4 E1 L4 97 25 BA 58 65 75 66 90 A4 5F A5 99 44 19 BE 25 25 F2 A5 P4 15 F0 32 55 75 44 A7 CF EC E2 45 75 89 77 67 20 41 75 75 78 44 75 68 D9 80 35 78 45 78 45 99 41 19 BE 25 25 F2 A5 P4 15 F0 70 55 75 44 A7 CF EC E2 45 45 78 78 97 76 75 94 77 75 75 84 75 68 D9 80 35 78 45 78 45 99 41 29 BE 25 25 78 45 P4 15 F0 70 55 75 44 A7 CF EC E2 45 45 78 78 78 77 CF 30 59 14 75 75 78 24 47 75 85 80 78 75 75 78 14 75 75 88 15 78 15 80 78 75 75 78 14 75 75 88 15 78 15 80 75 75 75 78 14 75 75 78 14 75 75 75 75 74 75 75 78 14 75 75 75 78 14 75 75 75 78 14 75 75 75 78 14 75 75 75 75 75 75 75 75 75 75 75 75 75</cyptool-en.btr,>			
Correlation of the second seco		$ \begin{array}{c} \begin{array}{c} a_{n} & b_{n} & b_{n} & a_{n} & b_{n} \\ e & p & q & q & q & h & b_{n} & a_{n} & 0 \\ 1 & (1, 1) & (1, 1) & (1, 1) & (1, 1) & (1, 1) & (1, 1) & (1, 1) \\ 0 & (1, 1) & (1, 1) & (1, 1) & (1, 1) & (1, 1) & (1, 1) \\ 0 & (1, 1) & (1, 1) & (1, 1) & (1, 1) & (1, 1) & (1, 1) \\ 0 & (1, 1) & (1, 1) & (1, 1) & (1, 1) & (1, 1) & (1, 1) \\ 0 & (1, 1) & (1, 1) & (1, 1) & (1, 1) & (1, 1) & (1, 1) \\ 0 & (1, 1) & (1, 1) & (1, 1) & (1, 1) & (1, 1) & (1, 1) \\ 0 & (1, 1) & (1, 1) & (1, 1) & (1, 1) & (1, 1) & (1, 1) \\ 0 & (1, 1) & (1, 1) & (1, 1) & (1, 1) & (1, 1) & (1, 1) \\ 0 & (1, 1) & (1, 1) & (1, 1) & (1, 1) & (1, 1) & (1, 1) \\ 0 & (1, 1) & (1, 1) & (1, 1) & (1, 1) & (1, 1) & (1, 1) \\ 0 & (1, 1) & (1, 1) & (1, 1) & (1, 1) & (1, 1) & (1, 1) \\ 0 & (1, 1) & (1, 1) & (1, 1) & (1, 1) & (1, 1) & (1, 1) \\ 0 & (1, 1) & (1, 1) & (1, 1) & (1, 1) & (1, 1) \\ 0 & (1, 1) & (1, 1) & (1, 1) & (1, 1) & (1, 1) \\ 0 & (1, 1) & (1, 1) & (1, 1) & (1, 1) & (1, 1) \\ 0 & (1, 1) & (1, 1) & (1, 1) & (1, 1) \\ 0 & (1, 1) & (1, 1) & (1, 1) & (1, 1) & (1, 1) \\ 0 & (1, 1) & (1, 1) & (1, 1) & (1, 1) & (1, 1) \\ 0 & (1, 1) & (1, 1) & (1, 1) & (1, 1) \\ 0 & (1, 1) & (1, 1) & (1, 1) & (1, 1) \\ 0 & (1, 1) & (1, 1) & (1, 1) & (1, 1) \\ 0 & (1, 1) & (1, 1) & (1, 1) & (1, 1) \\ 0 & (1, 1) & (1, 1) & (1, 1) & (1, 1) \\ 0 & (1, 1) & (1, 1) & (1, 1) & (1, 1) \\ 0 & (1, 1) & (1, 1) & (1, 1) & (1, 1) \\ 0 & (1, 1) & (1, 1) & (1, 1) & (1, 1) \\ 0 & (1, 1) & (1, 1) & (1, 1) & (1, 1) \\ 0 & (1, 1) & (1, 1) & (1, 1) & (1, 1) \\ 0 & (1, 1) & (1, 1) & (1, 1) & (1, 1) \\ 0 & (1, 1) & (1, 1) & (1, 1) \\ 0 & (1, 1) & (1, 1) & (1, 1) \\ 0 & (1, 1) & (1, 1) & (1, 1) \\ 0 & (1, 1) & (1, 1) & (1, 1) \\ 0 & (1, 1) & (1, 1) & (1, 1) \\ 0 & (1, 1) & (1, 1) & (1, 1) \\ 0 & (1, 1) & (1, 1) & (1, 1) \\ 0 & (1, 1) & (1, 1) & (1, 1) \\ 0 & (1, 1) & (1, 1) & (1, 1) \\ 0 & (1, 1) & (1, 1) & (1, 1) \\ 0 & (1, 1) & (1, 1) & (1, 1) \\ 0 & (1, 1) & (1, 1) & (1, 1) \\ 0 & (1, 1) & (1, 1) & (1, 1) \\ 0 & (1, 1) & (1, 1) & (1, 1) \\ 0 & (1, 1) & (1, 1) \\ 0 & (1,$		

3. Repeat step 1 using the same key. Plaintext shows up on the right.