Assignment 4

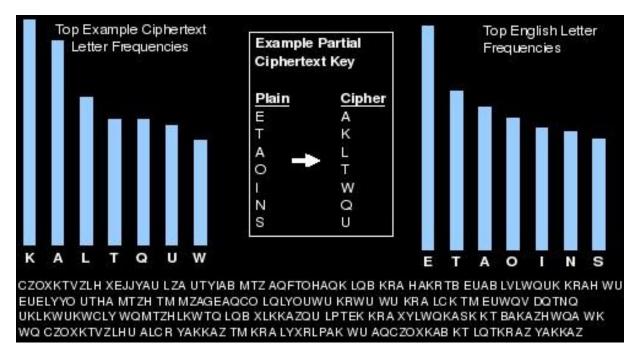
Task 1: Frequency Analysis (100 points)

The cryptanalyst can benefit from some inherent characteristics of the plaintext language to launch a statistical attack. For example, we know that the letter E is the most frequently used letter in English text. The cryptanalyst finds the mostly-used character in the ciphertext and assumes that the corresponding plaintext character is E. After finding a few pairs, the analyst can find the key and use it to decrypt the message. To prevent this type of attack, the cipher should hide the characteristics of the language. Table 1 contains frequency of characters in English.

Letter	Frequency	Letter	Frequency	Letter	Frequency	Letter	Frequency
Е	12.7	Н	6.1	W	2.3	K	0.08
Т	9.1	R	6.0	F	2.2	J	0.02
А	8.2	D	4.3	G	2.0	Q	0.01
0	7.5	L	4.0	Y	2.0	Х	0.01
Ι	7.0	C	2.8	Р	1.9	Z	0.01
N	6.7	U	2.8	В	1.5		
S	6.3	М	2.4	V	1.0		

Table 1 Frequency of characters in English

Cryptogram puzzles are solved for enjoyment and the method used against them is usually some form of frequency analysis. This is the act of using known statistical information and patterns about the plaintext to determine it. In cryptograms, each letter of the alphabet is encrypted to another letter. This table of letter-letter translations is what makes up the key. Because the letters are simply converted and nothing is scrambled, the cipher is left open to this sort of analysis; all we need is that ciphertext. If the attacker knows that the language used is English, for example, there are a great many patterns that can be searched for. Classic frequency analysis involves tallying up each letter in the collected ciphertext and comparing the percentages against the English language averages. If the letter "M" is most common then it is reasonable to guess that "E"-->"M" in the cipher because E is the most common letter in the English language. These sorts of clues can be bounced off each other to derive the key and the original plaintext. The more collected cipher text the attacker has, the better this will work. As the amount of information increases, its statistical profile will draw closer and closer to that of English (for example). This sort of thing can also be applied to groups of characters ("TH" is a very common combination in English for example). The example frequency analysis image above was performed on the first three sentences of this paragraph turned into a cryptogram. As you can see, the English language is very predictable with regard to letter frequency and this can exploited in some situations to break ciphers.



The goal of this lab is to gain a better understanding of a statistical attack by programming some of the important components to analyze/manipulate arrays of characters.

Lab Questions

- 1. What type of cipher is this program useful for breaking?
- In this type of cipher, the relationship between characters in the plaintext and characters in the ciphertext is ______.
- 3. List the frequencies for the top 4 characters found in the given ciphertext:

MKLAJZHAIUQWKHJABZNXBVHAGKFASDFGALQPIWRYIOQYWIERMASVZMNBZXCKJASDFGLKJFH WQERYIOQWTYIOASUDYFLASKJDHFZMZVBCXMVQLWERYIQRASDFQIWUERYIHKMFMAKHLSDFY UIOQWYREIORYIWQEUFHAKDFHLKASHFKVBBBNASMDFSADFWQEUYRUUEYRUUUQKASJHFKJDS HFSNBNBNBABABAAASKJFHLKJSADHFIDUASFOYDASIYFQWERBQWBRKLJLKASSADFDFDASDA

4. Break the cipher text given in the following. What is the plaintext? What is the key?

OTWEWNGWCBPQABIZVQAPMLJGZWTTQVOBQUMAPMIDGZCAB

EQVBMZLZIXMLAXZQVOQVLMMXAVWEIVLLIZSNZWAB

JQZLWNLMTQOPBVIUMLGWCBPAEQNBTGTMNBBPMVMAB

ITIAKWCTLVBBQUMQBEPQTMQBEIAQVUGBZCAB

What To Turn in:

A zip file named lastname_firstname_Assignment3.zip, containing:

- Source code
- A text file or Word document containing yours answers to the Lab Questions
- If you changed any other files in your project, please include them as well

Task 2: Lab on encryption using binary/byte addition (practice)

Under this encryption algorithm, the key entered is added character by character (byte by byte) to the data to be encrypted. Here addition modulo 256 is used, i.e. so that any carry-overs are ignored. The key is applied cyclically (as under the Vigenère encryption algorithm and also with the Exclusive-OR), i.e. once all the characters (bytes) of the key have been used, the algorithm reverts to the first character until the text has been completely encrypted.

To decrypt the text, the characters of the key have to be subtracted from the encrypted text modulo 256.

If one knows the characters which occur most frequently in the plaintext, it is then possible to work out the key with the aid of a computer (and hence also the plaintext) (see Automatic analysis, Byte Addition).

The key used for Binary Addition is entered in the Key entry dialog.

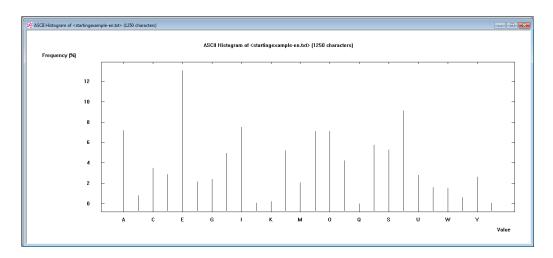
This encryption algorithm can be easily broken with a Ciphertext-Only attack (see Automatic analysis, Byte Addition). An example of this will be found in the Examples chapter.

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

9	CrypTool 14.30 - startingexample-en.bt
Ī	jile Edit View Engrypt/Decrypt Digital Signatures/[2KI Indiv. Procedures Analysis Options Window Help
ļ	
ſ	👫 startingeample-en.tz 💼 🖸 💌
l	CrypTool (Starting example for the CrypTool version family 1.x)
	CrypTool is a comprehensive free educational program about cryptography and cryptanalysis offering extensive online help and many visualizations.
	This is a text file, created in order to help you to make your first steps with CrypTool.
L	1) As a first step it is recommended you read the included online help, this will provide a useful oversight of all available functions within this application. The starting page of the online help can be accessed via the menu "Help > Starting Page" at the top right of the screen or using the search keyword "Starting page" within the index of the online help. Press F1 to start the online help expendence in the online help.
	2) A possible next step would be to encrypt a file with the Caesar algorithm. This can be done via the menu "Crypt/Decrypt -> Symmetric (Classic)".
	3) There are several examples (tutorials) provided within the online help which provide an easy way to gain an understanding of cryptology. These examples can be found via the menu "Help a Scenarios (Tutorials)"
	4) You can also develop your knowledge by: - Navigating through the menus. You can press F1 at any selected menu item to get further information. - Reading the included Readme file (set the menu "Help > Readme"). - Versing the included coloring in the presentation (This presentation can be found on several ways: e.g. in the "Help" menu of this application, or via the "Documentation" section found at the "Starting" page of the online help). - Versing the included color log.
	July 2010 The CrypTool team
L	

2. Click "Analysis\Tools for Analysis\Histogram".

St CrypTool 1.4.30 - startingexample-en.txt		Braulation day 70	and had a
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures	Analysis Options Window Help		
	Tools for Analysis	Entropy	
(*********************************	Symmetric Encryption (classic) Symmetric Encryption (modern) Asymmetric Encryption Hash Asymetric Encryption Hash ChypTol. In will provide a usaful oversight of all av I "Starting page" within the index of the o hm. This can be done via the menu "Cry which provide an easy way to gain an uncu	Floating Frequency Histogram N-Gram Autocorrelation Periodicity alable functions within this application nime help. pt/Decrypt -> Symmetric (Classic)". Herstanding of cryptology. These exart	
The CrypTool team			



We can see from the histogram that the character which occurs most frequently is the letter E. This is true of many German and English texts. This information will be used later on during our attack.

3. Close the histogram dialog. Choose from menu "Encrypt/Decrypt\Symmetric\Byte Addition".

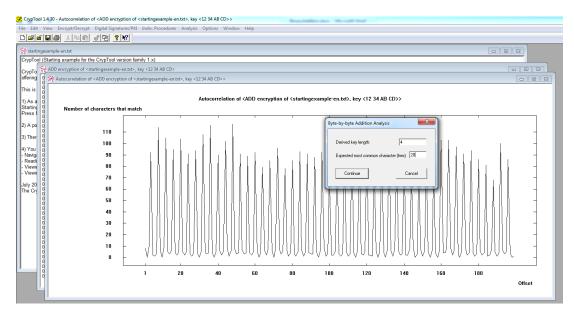
Key Entry: byte by byte addition (ADD)	×
Enter the key using hex characters (09, AF). Key length at maximum-2048 hex characters (= 1024 bytes).	
12 34 AB CD	6
<u>Encrypt</u>	<u>C</u> ancel

4. Enter **12 34 AB CD** as the key and click **Encrypt**.

The encrypted message shows up:

Civproor 1	130 - ADD encryption of <startingexample-en.txt>, key <12 34 AB CD></startingexample-en.txt>	
	ew Encypet/Decrypet Digital Signatures/EMI Indiv. Procedures Analysis Options Window Help	
6		
startinge	ample-en.txt	
~ _	arting example for the CrypTool version family 1.x)	
	ADD encryption of <startingexample-en.txt>, key <12.34 AB CD></startingexample-en.txt>	- • •
As a constraint of the second		$\begin{array}{cccccccccccccccccccccccccccccccccccc$

5. cipher text only attack will be performed. Choose from menu "Analysis\Symmetric\Ciphertext-only\Byte Addition".

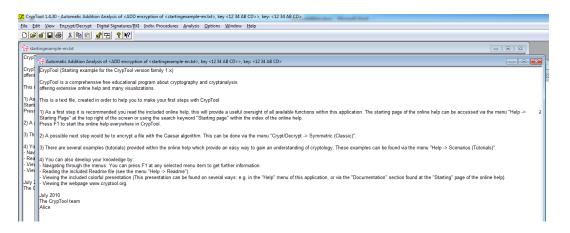


We are told that key length is calculated to be 4. The commonest character is E with hexadecimal value of 45. If we look at the plaintext, the most frequently character is e with hexadecimal value of 65. We enter into the Expected most common character field in the Byte-by-byte Addition Analysis box 20 (=65-45).

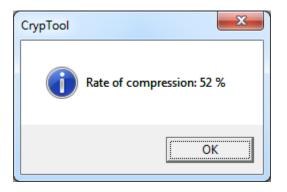
6. Click **"Continue**", CrypTool has been able to find the key. The only information was needed to do this was the fact that the character which occurred most frequently in the plaintext was the lower case letter e.

Byte-by-byte Addition Analysis	×
Derived key:	
12 34 AB CD	*
Decrypt	<u>C</u> ancel

7. Click the "**Decrypt**" button shows the plaintext.



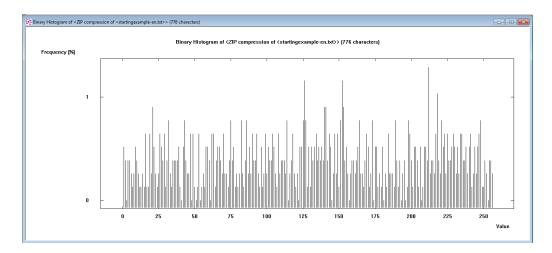
8. If the text is compressed prior to encryption then we will not be able to draw any conclusions from the frequency distribution of the characters in the text about the frequency distribution of the compressed text, since the compression process not only reduces size of a file but alters the frequencies of the individual characters so that they no longer reflect the frequencies of the characters in the original text. To compress the document, we make startingexample-en.txt active again. And select **"Indiv. Procedure\Tools\Compress\Zip**", the rate of compression is displayed.



9. Click "OK", the compressed document is shown.

CrypTool 1.4.30	0 - ZIP compression of <startingexample-en.bt></startingexample-en.bt>	ا م ا
	Encypt/Decrypt Digital Signaturer/PQ Indiv. Procedures Analysis Options Window Help	
CrypTool (Star	The compression of <starbingexample-en.bx></starbingexample-en.bx>	
CrypTool is a c offering extens	100000027 45 0A 24 65 45 7D 7D 67 29 4B BI EL F6 66 D3 CB D9 D9 D9 19 FA 21 8C DD B3 F7 96 A5 EF 9E 12 87 64 5C 4D F2 CA 6D 67 85 E. 5eBj0jK. f. l. d.M. seg 1000000075 20 42 52 F5 25 27 DC 64 B5 D6 76 5D 56 77 BE 76 B4 42 5A 26 5D D5 F2 BB 89 C4 54 FA B6 0B D2 80 8B E60 08 C. 3Pj. h. t. j. M. T. 100000075 20 42 52 F5 25 27 DC 64 B5 DF 07 5E 05 67 78 E7 B5 44 25 A2 E6 3D E8 9A 51 D8 55 03 1A 37 08 C2 & AE 57 7E BF 97 30 D00000075 20 44 74 44 F7 A4 F7 AC 14 26 DD B2 DF 69 D9 80 74 30 B4 67 6B FE E4 22 71 AB A6 59 E1 BD CC 98 C12 2E D3 DE 68 B9 60 C12 AE 30 C12 AB 30 C	
This is a text fi 1) As a first ste		
Starting Page" Press F1 to st	00000186 00 76 F4 E5 46 F7 93 47 B4 98 43 20 D5 38 34 12 14 E7 7C 51 B7 58 14 75 3E 46 A3 C2 39 75 42 DE D6 E0 7B 58 E 97 00v. F. G. C. 84[0.X.wF. 9uB[0000011AD 15 97 5D 97 D7 89 A2 EC DE DC 7B 96 C8 01 DA D7 3E E0 AC 55 55 A1 F3 51 B5 CA A3 FD 39 62 DA 39 BD 7F 94 09 4E A5 1B	
2) A possible r 3) There are se	00000222 DE 9A 1F C7 DB 7B 5C FA 9F 23 4A 71 L 6C 07 D3 E7 65 E9 34 D8 A7 0D FD 65 ED 15 04 69 9E 24 CC 66 7D 37 65 EA C5 F9	
4) You can als - Navigating the - Reading the i	00000277 52 97 43 75 19 13 75 44 44 40 19 14 #74 52 5C 54 97 14 189 34 65 5C 59 76 97 189 55 55 19 97 65 15 55 19 74 18 74 55 14 14 14 19 14 #74 52 5C 55 19 14 19 14 14 14 14 14 14 14 14 14 14 14 14 14	
- Viewing the in - Viewing the v		
July 2010 The CrypTool t		

10. Click **"Analysis\Tools for Analysis\Histogram**" to see its histogram. The compression produces a quite different histogram profile from the one previously obtained for the uncompressed document. The characters are much more evenly distributed than in the unencrypted document.



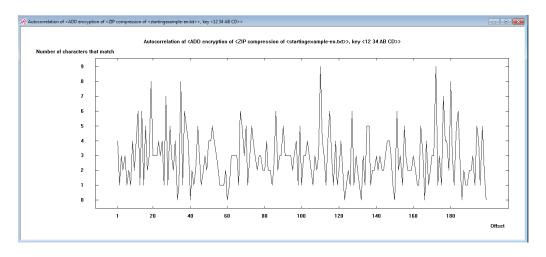
11. Make the compressed document the active window once again and the encrypt it using the same key **12 34 AB CD**.

Key Entry: byte by byte addition (ADD)	X
Enter the key using hex characters (09, AF). Key length at maximum-2048 hex characters (= 1024 bytes).	
12 34 AB CD	6
<u>Encrypt</u> <u>D</u> ecrypt	Cancel

12. Click "Encrypt".

) 🗃 🖬 🗇 🗴 Pa 📾 🛷 🔁 🔋 😢	
Off-ADD encryption of <2DP compression of <statingeample-entits>, key <1234 AB CD> Off-ADD encryption of <2DP compression of <statingeample-entits>, key <1234 AB CD> 00000017 12 1 C 58 40 51 42 75 19 A8 42 44 67 E8 02 53 C1 07 D7 74 95 03 78 83 E4 E1 1A 46 00000017 12 1 C 58 40 51 42 75 19 A8 42 44 67 E8 02 53 C1 07 75 74 95 03 78 83 E4 E1 1A 46 00000007 12 1 C 58 40 12 87 E8 11 27 55 20 55 00 C3 78 00 75 64 E8 00 C4 73 30 C0 88 80 09 00000007 13 1 C 58 20 21 30 75 19 84 62 44 67 E8 00 53 C1 07 75 74 95 03 78 83 E4 E1 1A 46 00000075 83 7E F2 11 01 E0 1C 09 97 0C 59 4C 7A 00 38 41 42 E5 12 38 10 18 09 38 ED 05 14 41 45 59 27 E1 22 05 42 88 58 74 40 65 86 00000015 83 7E F2 11 01 E0 1C 09 97 0C 59 4C 7A 00 38 41 42 E5 12 38 10 18 09 38 ED 05 10 41 41 45 70 14 10 15 01 64 61 59 10 00 64 61 23 11 71 13 13 65 40 65 86 00000015 83 7E F2 11 01 E0 1C 07 97 07 25 04 76 C4 A4 C1 20 64 64 59 74 84 65 76 AD 00 64 61 23 10 71 13 13 65 64 64 69 75 84 00 50 64 64 13 65 86 65 64 65 66 66 65 66 66 65 66 66 66 66 66 66</statingeample-entits></statingeample-entits>	$ \begin{array}{cccccccccccccccccccccccccccccccccccc$

13. We invoke the analysis again by choosing from menu "Analysis\Symmetric\Ciphertext-only\Byte Addition".



CrypTool returns an incorrect key length of 12.

Byte-by-byte Addition Analysis	×
Derived key length:	12
Expected most common charac	cter (hex): 00
Continue	<u>C</u> ancel

Given this key length, it is not possible to find the correct key either.

14. We will check whether it is possible to arrive at a readable version of the text document from the compressed and then encrypted document. We will provide the key and then unzip.

We will make the compressed and encrypted document the active window again. Choose from menu "Encrypt/Decrypt\Symmetric\Byte Addition".

Key Entry: byte by byte addition (ADD)	×
Enter the key using hex characters (09, AF). Key length at maximum 2048 hex characters (= 1024 bytes).	
12 34 AB CD	6
<u>Encrypt</u> <u>D</u> ecrypt	<u>C</u> ancel

15. Enter **12 34 AB CD** as the key and click **Decrypt**.

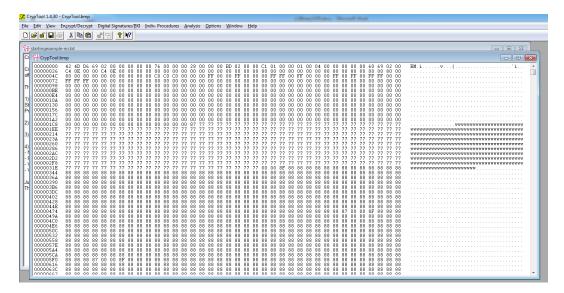
00000000	43 54 5A 75	55 41 6F	DB 30	10 BC 1	B E0 1	F 16 34	L C5 4	40 FÅ	36.6	9 4F	39 1	4 08	12 14	45	IE 45	D1 04	05 74	5C 4B 6B 89	08	CTZuUAn.0
00000027	45 0A 24 65	45 7D 7D			1 F6 6				19 F			Ď B3			9E 12			F2 CA 6D 67		E.\$eE}}g)K. f
0000004E	F6 3E 50 6A	84 1E E6	92 83			D B7 C6		74 B3	7D D		57 E		F2 BB			FA B6			8C	>Pih.=t.}.VT
00000075		25 27 DC				6 78 E			AE 2		E8 9		D8 55				26 AI			BR.%'.dK].uxD%.&=Up.&₩~
1000009C	71 4A 47 44 . 70 92 8A 8C	EF AC 71		D8 2E E	0F 68 I	9 8D 74 F 9F 5F			6B F		2E 7	1 AB	AC 9E		00 C9	8C 12 2C 2A	2E D: 64 FI		BC E4	qJGD.qB. h.t0.gk.q. X. p.#.*. ~B.}.[~.P.b.4.,*d. +
1000000EA		20 IF 28				9 7E 55			D2 F			2 FF	1A BF			59 97	83 4		7D	P. *.* B. /. [F. D * *u + V. & ~U. zz V }
00000111		EB 26 91	DF 13		F 6C 2		1 31 B		F3 Å	ŭ 99	19 6	ŝ ĉ9	30 DC	25 1	06 4C	3Å 6F	E9 19	2D E3 BC D0	8Ē	o.g. & 1, t1.+ f.0.u.L:o
0000138	6B 51 14 E5	71 2A 5F			9 96 1				1A F		A9 F		25 EF			8B 1F		88 53 AE 49	BE	kQ.q*vhY.#
000015F		83 08 6D	45 65	C5 00 5	A 9D 0	F 84 4	3 D9 I	D0 8B	8C 0	3 E4	A6 E	2 E9	94 51	F1 (C6 5E	E5 A9	E4 F	1F 1C A1 F6		.0
0000186	00 76 F4 E5 15 97 5D 97	46 F7 93 N7 89 A2	47 BA BC ED	98 43 2 EC 7B 9	10 D5 3	8 34 12 1 DA D3	2 14 E 7 3F F	27 7C. 30 AC.	51 B 55 5	7 58 5 A1	14 7 F3 5	5 3E 1 B5	46 A3 CA A3	C2	39 75 89 62	42 DE	D6 EI BD 71) 7B 5B E9 F0 7 94 09 4E A5		.v.F.G.C.84. Q.X.u>F.9uB. {[
100001D4	E1 85 14 4C			A2 DC 1		6 C7 81					F0 8		1C 73			F5 09				LIV A n 9 J h s * -
00001FB	54 AC D3 D9	37 Č6 40	É1 C5	3D 8E 8	4 E3 4	8 03 88		59 CD	B8 8	1 B3	1E E	à čž	Å 8 88	8B	BA OF	95 Å7	DC 59	5F 8F D9 2A		Т
0000222		DB 7B 5C	FA 9F	23 4A 7		C 07 D:			34 D		OD F.					2Å CC				{\#Jq4*.f}7e
0000249		EE C6 3B 80 82 94	5A AF	DE D1 7	7 3E 9	8 9A D3 7 AB 91			FB B		DA C B3 2		82 D4 24 FA			F7 34 D2 &F	ED 5: 22 D	. AC 94 1A E3 3 A9 CB 49 A7	4C 92	.J.3.;Zv>
0000270		50 82 94 19 19 2F	40 43	20 10 3	L 80 U	A 52 50			7E 2 8B 3		EC E		24 EA 57 70			55 C5				\$i
00002BE		92 13 71		6B CD I	BBC	8 E2 D:		7D 3B			9A 5					DC 15		0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	64	s.bbqk
00002E5		08 4E 6E	41 42	7C A8 F	3 96 E	F F5 78	FE 6	SF 3F	ĎĊ Ž		67 F	6 Ĕ4	0F 22	0.9 1	87 EB	D5 3D	98 C	SF		.k.a.Nnà. x.o?. .g=

16. Choose from menu "Indiv. Procedure\Tools\Compress\UnZip", and the original text is displayed.

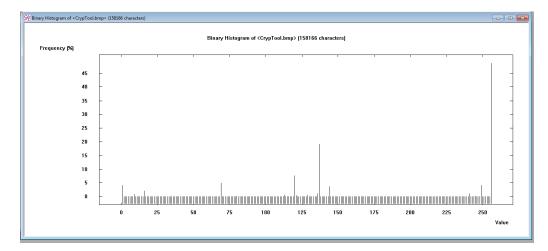
ie Edit Yiew Engrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help	
+ ZIP decompression of <add <add="" <startingexample-en.txt="" <zip="" compression="" decryption="" encryption="" of="">>, key <12 34 AB CD>>, key <12 34 AB CD>></add>	
CrypTool (Starting example for the CrypTool version family 1.x)	
CrypTool is a comprehensive free educational program about cryptography and cryptanalysis offering extensive online help and many visualizations.	
This is a text file, created in order to help you to make your first steps with CrypTool.	
1) As a first step it is recommended you read the included online help, this will provide a useful oversight of all available functions within this application. The starting page of the online help can be accessed via the i Starting Page ² at the top right of the screen or using the search keyword "Starting page" within the index of the online help.	menu "Help ->
2) A possible next step would be to encrypt a file with the Caesar algorithm. This can be done via the menu "Crypt/Decrypt -> Symmetric (Classic)".	
8) There are several examples (tutorials) provided within the online help which provide an easy way to gain an understanding of cryptology. These examples can be found via the menu "Help -> Scenarios (Tutorials)".	
t) You can also develop your knowledge by: Navjating through the menus. You can press F1 at any selected menu item to get further information. Reading the included Readme file (see the menu "help -> Readme"). Viewing the hebrage www cryptool org.	ielp).
July 2010 In CrypToleam Nice	

Task 3: Encryption using binary Exclusive-OR (XOR) (practice)

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



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



You can see from the histogram that the character which occurs most frequently has the value **255**. In hexadecimal notation this corresponds to **FF**. This information will be used later on during our attack.

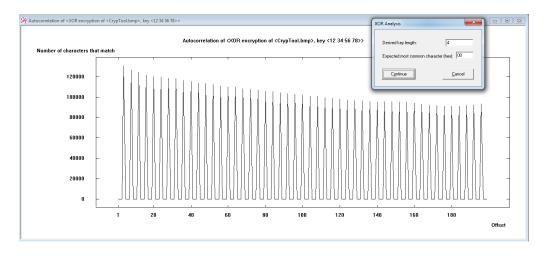
3. Click on the window of "CrypTool.bmp". And click "Encrypt\Decrypt/Symmetric/XOR" from menu.

Key Entry: byte by byte XOR	X
Enter the key using hex characters (09, AF). Key length at maximum 2048 hex characters (= 1024 bytes).	
12 34 56 78	3
Encrypt Decrypt	<u>C</u> ancel

- 4. Enter **12 34 56 78** as the key.
- 5. Click "Encrypt"

ST XOR encryption of <cryptool.bmp>, key <12 34 56 78></cryptool.bmp>	
000000000 16 7 9 11 13 4 6 7 12 34 6 7 12 34 6 7 12 34 6 7 12 34 6 7 12 34 56 7 12 34 56 7 12 34 57 7 12 34 57 12 34	Py 4 Vx 4 x

6. We will perform the cipher-text only attack. Select "Analysis\Symmetric Encryption\Ciphertext-Only\XOR".



The autocorrelation is calculated and displayed. We are told that the key length is calculated to be 4. As we have seen in step 2, the most commonest character is FF. This we enter in the **Expected most common character field**.

XOR Analysis	X
Derived key length:	4
Expected most common chara	icter (hex): FF
Continue	<u>C</u> ancel

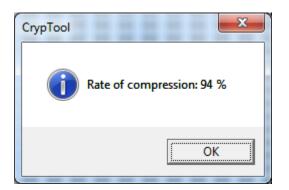
7. Click "Continue".

XOR Analysis	x
Derived key	:
12 34 56 78	* *
ecrypt	<u>C</u> ancel

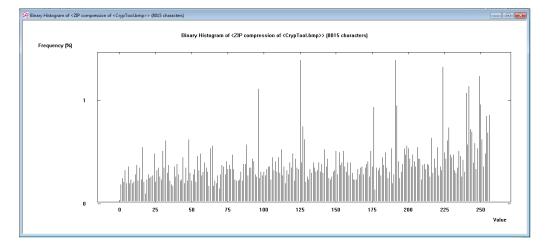
8. Click "Decrypt".

Edit ⊻iew	 Engry 	pt/Decryp	t Digita	I Signati	ures/PK	l Indiv	r. Proced	dures	Analysis	Qptions	Wind	ow ∐	elp								
2 🖌 🖌	6	6 🖻 📾	89	al የ	2																
				<u> </u>		_	_	_				_			_	_		_	 _		
Automati	ic XOR A	nalysis of •	XOR end	ryption	of <cry< th=""><th>pTool.b</th><th>pmp>, k</th><th>ey <12</th><th>34 56 78></th><th>>, key: <1</th><th>2 34 56 7</th><th>8></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th></cry<>	pTool.b	pmp>, k	ey <12	34 56 78>	>, key: <1	2 34 56 7	8>									
00000000 00000252 00000072 0000072 0000072 0000072 00000072 00000000	C4 FF 000 000 000 000 000 000 000 000 000	00 00 0 0 00 00 00 0 0 000 00 00 0 0 0 000 00 0 0 0 0 0 000 00 0 0 0 0 0 0 000 00 0 0 0 0 0 0 0 000 00 0		$ \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 &$	00 000 000	00 00 00 00 00 00 00 00 00 00 00 00 00		000 000 000 000 000 000 000 000 000 00		00 00 00 <	00 00 00 FF 00 00 FF 00 00 00 00 00 00 00 00 00 00 00 00 00			0 00 0 00 00 0 00 0 0 0 0 0 0 0 0 0 0		00 000	00 800 800 FF 00 0<	000 F00 F000 F000 F000 F000 F0000 F0000 </td <td>0 0 00 00 00 00 00 00 00 00 00 00 00 00</td> <td>$\begin{array}{cccccccccccccccccccccccccccccccccccc$</td> <td>EH 1</td>	0 0 00 00 00 00 00 00 00 00 00 00 00 00	$ \begin{array}{cccccccccccccccccccccccccccccccccccc$	EH 1

9. If we compress the document before encryption. By clicking "Indiv. Procedure\Tools\Compress\Zip".



10. Select "Analysis\Tools for Analysis \ Histogram", which produces a quite different histogram from the one previously obtained for the uncompressed picture in bitmap format.



11. Encrypt the compressed document by selecting "Encrypt\Decrypt/Symmetric/XOR" from menu and use **12 34 56 78** as the key.

12. We will perform the analysis. Select "Analysis\Symmetric Encryption\Ciphertext-Only\XOR". CrypTool returns incorrect key length.