

Lab-Encryption Methods

1. The encrypted message : VECIHXEJZXMA , Cipher : TCP/IP , Decrypted: CCNASECURITY
2. The encrypted message : RIYXIG , Cipher : CEH , Decrypted:
3. The encrypted message : ESUIVHVW , Cipher: CEH , Decrypted :

	B	C	D	E	F	G	H	I	J	K	L	M	N
T	C	P	I	P	T	C	P	I	P	T	C		
V	E	C	I	H	X	E	J	Z	X	M	A		
C	C	N	A	S	E	C	U	R	I	T	Y		
C	E	H	C	E	H								
R	I	Y	X	I	G								
P	E	R	V	E	Z								
C	E	H	C	E	H	C	E						
E	S	U	I	V	H	V	W						
C	O	N	G	R	A	T	S						

<https://sharkysoft.com/vigenere/1.0/>

This page is for amusement only. Instructions are given below this form.

Input: clear	VECIHXEJZXMA
Key: clear	TCP/IP
Coding direction:	encode decode
Output: clear	CCNASECURITY

https://sharkysoft.com/vigenere/1.0/

This page is for amusement only. Instructions are given below this form.

Input: clear	RIVXIG
Key: clear	CEH
Coding direction: encode decode	
Output: clear	PERVEZ

https://sharkysoft.com/vigenere/1.0/

This page is for amusement only. Instructions are given below this form.

Input: clear	ESUIVHVW
Key: clear	CEH
Coding direction: encode decode	
Output: clear	CONGRATS

1. Could the Vigenère cipher be used to decode messages in the field without a computer?

- Yes, with the help of cipher text and Vigenere cipher square.

2. Search the Internet for Vigenère cipher cracking tools. Is the Vigenère cipher considered a strong encryption system that is difficult to crack?

- No, there are many tools available on the internet for cracking.
-

Lab-Feistel Cipher:

- a) What is the Function used in the book?

- It uses a round function, a function which takes two inputs, a data block and a subkey, and returns one output the same size as the data block. In every round, the round function is run on half of the data to be encrypted and its output is XOR with the other half of the data.

- b) How many rounds did they go?

- 16 rounds are performed in the Feistel cipher. The number of rounds also increases the security of the block cipher. More is the number of rounds is the cipher.

- c) Can you put a python implementation? What library did you use?

- Yes, we can implement Feistel cipher on python.

```
# Python program to demonstrate
# Feistel Cipher Algorithm

import binascii

# Random bits key generation
def rand_key(p):
    """
    """
    import random
    key1 = ""
    p = int(p)
    for i in range(p):
        temp = random.randint(0,1)
        temp = str(temp)
        key1 = key1 + temp
    return(key1)

# Function to implement bit xor
def exor(a,b):
    """
    """
    temp = ""
    for i in range(n):
        if (a[i] == b[i]):
            temp += "0"
        else:
            temp += "1"
    return temp

# Defining BinarytoDecimal() function
def BinaryToDecimal(binary):
    """
    # Using int function to convert to
    # string
    """
    string = int(binary, 2)
    return string
```

```
# Feistel Cipher
PT = "Hello There"
print("Plain Text is:", PT)

# Converting the plain text to
# ASCII
PT_Ascii = [ord(x) for x in PT]

# Converting the ASCII to
# 8-bit binary format
PT_Bin = [format(y,'08b') for y in PT_Ascii]
PT_Bin = "".join(PT_Bin)

n = int(len(PT_Bin)//2)
L1 = PT_Bin[0:n]
R1 = PT_Bin[n:]
m = len(R1)

# Generate Key K1 for the
# first round
K1= rand_key(m)

# Generate Key K2 for the
# second round
K2= rand_key(m)

# first round of Feistel
f1 = exor(R1,K1)
R2 = exor(f1,L1)
L2 = R1

# Second round of Feistel
f2 = exor(R2,K2)
R3 = exor(f2,L2)
L3 = R2

# Cipher text
bin_data = L3 + R3
str_data = ''
```

```
# Cipher text
bin_data = L3 + R3
str_data = ''

for i in range(0, len(bin_data), 7):
    # slicing the bin_data from index range [0, 6]
    # and storing it in temp_data
    temp_data = bin_data[i:i + 7]
    # passing temp_data in BinaryToDecimal() function
    # to get decimal value of corresponding temp_data
    decimal_data = BinaryToDecimal(temp_data)
    # Decoding the decimal value returned by
    # BinaryToDecimal() function, using chr()
    # function which return the string corresponding
    # character for given ASCII value, and store it
    # in str_data
    str_data = str_data + chr(decimal_data)

print("Cipher Text:", str_data)

# Decryption
L4 = L3
R4 = R3

f3 = exor(L4, K2)
L5 = exor(R4, f3)
R5 = L4

f4 = exor(L5, K1)
L6 = exor(R5, f4)
R6 = L5
PT1 = L6 + R6

PT1 = int(PT1, 2)
RPT = binascii.unhexlify( '%x' % PT1)
print("Retrieved Plain Text is: ", RPT)
```

```
Plain Text is: Hello There
Cipher Text:  (9\,fH2
Retrieved Plain Text is:  b'Hello There'
```

A)

Cracking Caesar Shift Cryptography:

Cryptography is a form of security that will simply be going to convert the introductory text into ciphertext. This process makes simple, readable text into a coded form that can only be read by decoding it. That is the main reason cryptography and encryption are known to be one of the best ways to protect data. However, it is also essential to know how to crack the Cesar shift cryptography.

This can be explained as one of the most accessible encryption algorithms the Latin a letter uses and simply shifts to the confidence of the set. Moreover, it can also have the opportunity and alphabet that will be used just by the 26 Latin letters for cracking or encryption. This is the only way to help create an alphabet that will rotate exactly by it. Moreover, that is the way cracking Caesar's cipher is done.

Background Of Caesar Cipher Cryptography

Any small or major change in the message but going to prevent it from any unauthorized reading. This can only be done with the help of end-to-end encryption, which will be going to keep

the secret codes only with you and your close ones. Further, it will solve the secret code that is used to secure communication and other files. This is the way by which most of the ciphertext is also known as secure text.

Conclusion

From the past few years, we have seen tremendous growth and development in the information technology sector. Not only this, but it has also created a completely new market, that is why it is very important to know the background of how the secret works and what is used for secure communication. Moreover, it is also very important to crack the seizure shift cryptography that will work after the very known cipher.

History of AES from DES:

Introduction

In cryptography, the data and information encryption standard plays a significant role because it is the only standard that will provide a secure environment for converting the introductory text into ciphertext. That is why it is essential to know the one encryption standard that will rule out all the other encryption standards. After analyzing all the encryption standards, the advanced encryption standard is one of the most widely used encryption algorithms. The primary reason the advanced encryption standard is widely used is that the application of AES includes the encryption of the data at rest. This will further provide a symmetric encryption algorithm that was developed to use for facto encryption standards.

AES Encryption Algorithm

One of the most widely used encryption standards is the advanced encryption standard. This algorithm will create a much more secure environment for the primary data as it will help classify the encryption of all the electronic data. Apart from this, it will also adopt the suspenders of data in corruption standards and other algorithms, which will have the symmetric key for both encrypting and decrypting the information or data.

However, it also has the block passed from the sequel of the steps to the total times, so it is essential to include it in the security. The simple key of advanced encryption standard will be a computer process with a new key for the following rounds.

Conclusion

In the current scenario securing the data is very important, and the best way to secure the written information is by encrypting the complete information. That is why choosing the correct data on corruption is essential, which will rule all the other standards. Therefore, the advanced

encryption standard is currently one of the most systematic block ciphers to protect all classified and sensitive information.

Data Encryption Standard:

Introduction

In the video, the discussion was about data encryption standards. It will create a more secure environment for the primary written text to convert into Cypher text. However, the data encryption standard can be explained and found in the vulnerable against a very powerful attack that can breach the system security. That is the main reason DES is used in the popularity found if there is any decline. Moreover, it will also be going to help in creating encryption data in a block of size.

Therefore, the data encryption standard will act as a symmetric key algorithm for encrypting any digital data or information. It will protect it from any uncertain or unauthorized access and convert the data into ciphertext to not be readable by any invader.

General Structure Of Data Encryption Standard

The data encryption standard will provide a symmetric key block cipher published by the National Institute of Standards and technology, which will have the structure DES. Moreover, it will also have its illustration that will be initial permutation, Around function key generalization, and DES analysis. These are the general standards of data encryption that will transform the basic and straightforward data into ciphertext.

Conclusion

This study talks about cryptography and its data encryption standard, which will provide a symmetric key algorithm for encryption. Further, it will be going to protect the Digital data that will have to create an insecure application that is highly influential and advancement for cryptography. This way, it will have the algorithm, which will be submitted to the national bureau of standards for inviting the purpose of protecting the sensitive and classified data. The protection of the data is much more reliable with encryption.

Triple DES:

Introduction

In cryptography, there is the term known as triple data encryption algorithm. It can be simplified as a systematic key block cipher that will apply in the algorithm three times to each Data block. This will further be going to provide a more secure system and convert the simple text into ciphertext. However, it is essential to know the triple data encryption standard, which is an easy modification of the existing software as it is done simply by the algorithms.

Before applying encryption in any confidential or sensitive data, it is very important to overlook the encryption standards. It is because this is the only way that will be going to help in replacing the encryption with advanced high-level encryption standard, which is more secure. For that, it is very important to understand the triple data encryption standard.

Triple Data Encryption Standard Algorithm

For a better understanding of the triple-DES, it is very important to understand what its algorithm is. It can be simplified as another mode of data encryption standard operation; however, it takes 64-bit K_i and the overall 129-bit key length. That is why it runs three times slower than the data encryption standard, but it is more secure if used properly. Further, it also has different modes like electronic codebook Sai for book training and much more. This will be implemented as a methodology for the symbol or standard to the cipher block Chaining.

Conclusion

In the present scenario, most of the crucial data is available in the network. That is why it has become very important for people to understand the importance of security, and the best major for security is the data encryption standard. The data encryption standard will make a symmetric key block cipher which is applied in the algorithm three times to each block of data. This will enhance the protection, but the downside of this triple data encryption standard is that it will reduce the speed.

AES Encryption Work Advance Encryption Standard:

Introduction

Encryption is one of the essential parts of digital security at present. From the past few years, we have seen growth and development in the information technology sector. Apart from this, there have also been a few daily life application up-gradation that have created so much ease. However, all the information collected from multiple programs and applications is stored in a network server; however, the information is sensitive and crucial. That is why it is essential to have encryption. Data encryption will simply be going to create a simple text into ciphertext.

Moreover, it will also have an algorithm that will act as a data encryption algorithm for making and standardizing Abreaking into data encryption standards. However, it is essential to know about the advanced encryption standard. It is because this will be going to create a block cypher chain that will protect all the classified information. Further, it is vital to understand how the advanced encryption standard works.

Working on advanced encryption standard

For a better understanding of advanced encryption standards, it is essential to know how it works. It simply helps in learning how to transmit information between multiple steps. Not only this, but it will also have information about the single block. This will further be going to help in

solving the Matrix, which is known as state aery. The advanced encryption standard works with features like Key explanation, bite Data, key length and SP network.

Conclusion

Primarily one of the most important as it for every organization in the present scenario is Data. That is why data and information are some of the most crucial aspects of any organization. Therefore, it is essential to protect all the data from any uncertain access, and that can only be done by implementing all the necessary security features. This way, there will be a proper security standard, and it will all be standardized by encryption. Encryption will simply be going to help in changing the simple data into ciphertext. With the advanced capability of advanced encryption standards, there will be symmetric block Cypher to protect all the classified data.

Advanced Encryption Standard Explained:

Introduction

Whenever there is talk about cyber security, the advanced encryption standard will be one of the best steps that will pop everywhere. The primary reason behind the success of advanced encryption standards as it provides a global standard of encryption that will simplify the amount of communication and make it safer. Moreover, the advanced encryption standard works much faster and is secure from any other form of encryption.

That was the main reason why the advanced encryption standard has been developed. In the earlier stage of encryption, it simply uses the techniques that will help change the letter and the sentence further. It will completely change the simple text into ciphertext so that any unauthorized person cannot read it.

Securing information with Advanced Encryption Standard

In the present scenario, cybercrimes are increasing day by day, creating importance for protection. That is why data encryption has been used to completely secure the data from any unauthorized access. The best way is to use the Advanced Encryption Standard. Primarily it is a global or universal standard for encryption as well as it is in the most common way that will go to help in protecting sensitive data. Apart from this, the advanced encryption standard has a unique key that will decrypt the data to further be accessed. This is also why the advanced encryption standard or AES is the fastest publicly accessible ciphertext approved by national security agencies.

Conclusion

Data security is critical. That is why encryption has been used. For the advanced level of security, the advanced encryption standard is one of the most popping standards. This will not only help secure the data but also become a global standard for encryption that will keep the significant amount of communication much safer than any other form of encryption. That was the main reason the advanced encryption standard is used, as it is much faster and more secure than any other encryption type.

Public and Private Key Encryption:

Cryptography is a vast science of secret writing in computer technology. In the current scenario, most organizations and companies have vast data with crucial and confidential information. To protect that information from any invader, organizations use cryptography or corruption, which will simply be going to create the hash and encode and decode the writing so that there will be a keeping of data secret.

That is why it is essential to understand the difference between the private key and the public key that will help create secret writing and keep the data secure from any unauthorized access.

- **Private key:** in simple words, the private key can be explained as a secret key used to encrypt and decrypt the information or data. This uses a symmetric system because the only key is copied or shared by the party to decrypt the information. This is the reason why it is much faster than public-key cryptography.
- **Public key:** a public key is a cryptography. In simple words, it can be explained as encryption of writing but having two keys that will use the primary key for encryption and another key for decrypting that retain information. Therefore, the one key, also known as the public key, is used to encrypt the plain text and convert it into a cypher text so that no unauthorized access could be there. For further authentication, there is another key known as a private key that the receiver will use to decrypt that particular ciphertext.

Conclusion

Cryptography is essential for the protection of data, especially when cyberattacks are at their peak. However, before encrypting any data, it is essential to know what cryptography is and keep the data secure. Apart from this, it will also help understand the difference between private and public keys, which is a form of cryptography that is used for encryption and decryption of written data. This will convert the simple plain text into ciphertext.

Hashing Versus Encryption:

Introduction

This video is about hashing and encryption and its difference. Primarily it is essential to know what is hashing and its document for ensuring accuracy. It is essential to understand that there is a bit of a difference between hashing and encryption.

Hashing refers to the permanent data converted into a message. On the other hand, encryption works in two ways. For simple understanding, it can be explained as encryption will include and decode the data; however, hashing will help protect the integrity of the information that has been corrupted or coded.

The complete video is divided into two sections covering the document hashing to ensure accuracy and password hashing for increased security. Moreover, it also has the difference between hashing and encryption.

Difference Between Hashing and Encryption

For better understanding the difference, it is essential to know what individual terms mean. Hashing can be explained as changing the plain text or a key into a hash value. On the other hand, encryption is a process that will be going to secure all the sensitive and confidential information like username password, credit card details, banking details and other financial details away from the reach of hackers as it will going to simply in court and decode the information that is presented so that any invader could not understand the text. This is the primary difference between hashing and encryption.

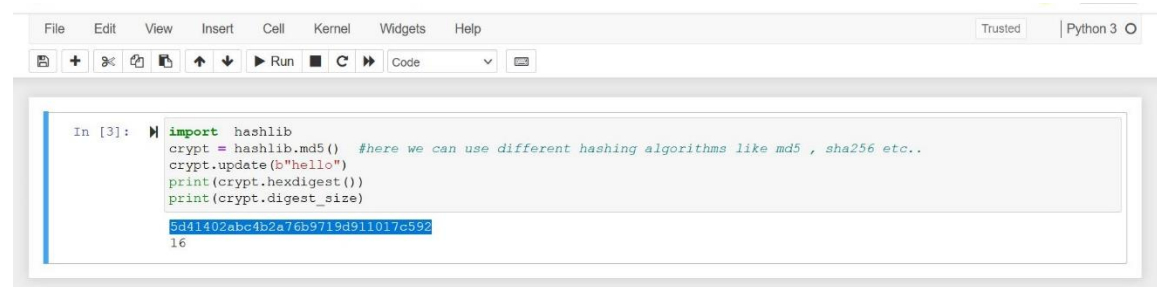
Conclusion

The video explains the type of accuracy check and the difference between hashing and encryption, which will be going to enhance the protection of the data. Moreover, it will also have the work with two different keys to provide the result in the collision. It works with the algorithm and creates a security measure for the information, which is compared with a huge amount of data. It is easy to keep records and find the records of the highest data. On the other hand, encryption will be divided into two categories: the model and the historical. Both will be going to symmetrically encrypt the data and create a security key which is also known as ciphertext, To protect the information.

B)

Advanced Encryption Standard is used to secure important data. It is a symmetric block cipher, and it is also used in both the hardware and the software across the countries to encrypt the important data. There are many advantages of Advanced Encryption Standard compared to others. Advanced Encryption Standard is quicker compared to other standard encryption such as Data encryption. Advanced Encryption Standard is more powerful compared to other standard encryption which results in lesser vulnerability from the attackers.

C)



```

In [3]: import hashlib
        crypt = hashlib.md5() #here we can use different hashing algorithms like md5 , sha256 etc..
        crypt.update(b"hello")
        print(crypt.hexdigest())
        print(crypt.digest_size)

5d41402abc4b2a76b9719d911017c592
16

```

D)

A rainbow table attack is a kind of hacking where the offender makes an attempt to use a rainbow hash table to split the passwords which are set aside in a database system. A rainbow table is a hash work used in cryptography for taking care of huge data like passwords in an informational collection. To avoid rainbow table attacks confidential and sensitive data is hashed twice with the same or with different keys

.

```

In [3]: import hashlib
        crypt = hashlib.md5() #here we can use different hashing algorithms like md5 , sha256 etc..
        crypt.update(b"hello")
        print(crypt.hexdigest())
        print(crypt.digest_size)

5d41402abc4b2a76b9719d911017c592
16

In [2]: import hashlib,binascii
        dk = hashlib.pbkdf2_hmac('sha256', b'password', b'salt', 100000)
        print(binascii.hexlify(dk))

b'0394a2ede332c9a13eb82e9b24631604c31df978b4e2f0fbd2c549944f9d79a5'

```

The number of *iterations* should be chosen based on the hash algorithm and computing power. As of 2013, at least 100,000 iterations of SHA-256 are suggested.

LAB AES:

Which of the 4 steps in AES uses confusion?

Subbytes

Shift rows

Mix Columns

Add Round Keys

Which of the 4 steps in AES uses diffusion?

Add Round key

Inverse Mix columns

Inverse Shift rows

Inverse Subtypes

1. Why does decryption in AES take longer than encryption?

Encryption must be done sequentially, while decryption can be parallelized as the XOR step (with the previous block of ciphertext) is done after the block cipher is applied. decryption is slower because an additional instruction, AES inversion mix columns, must be used every round.

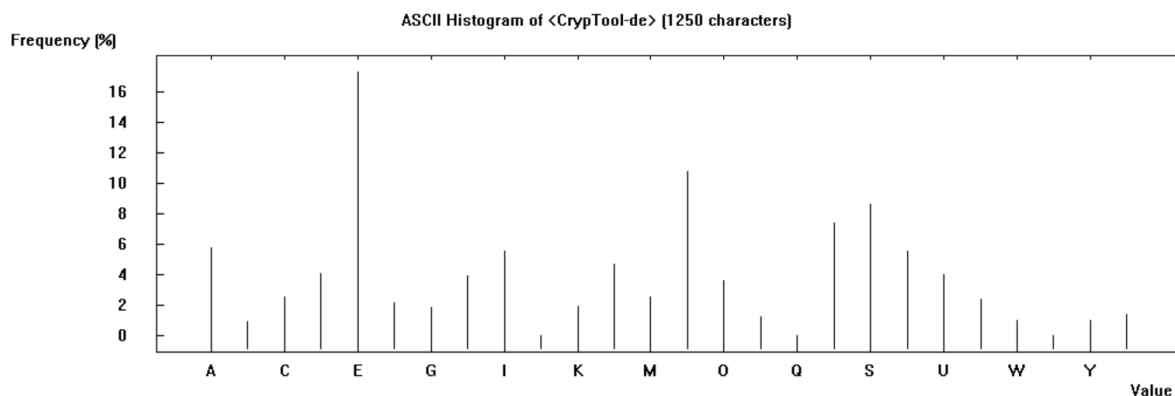
2. Describe the use of blocks and rounds in AES.

Using the AES key schedule, round keys are produced from cipher keys. Each round of AES requires a distinct 128-bit round key block, plus one extra.

3. Why would one want to increase the total number of Rounds in AES? For increase in the security

Lab-Binary Addition:

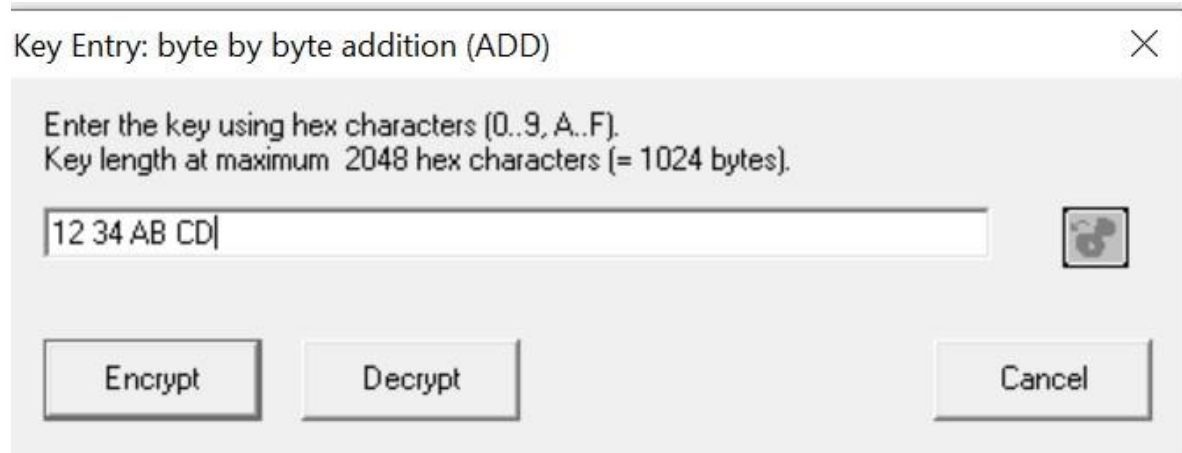
1. Open the file CrypTool-en.txt under C:\Program Files (x86)\CrypTool\examples.
2. Click “Analysis\Tools for Analysis\Histogram”



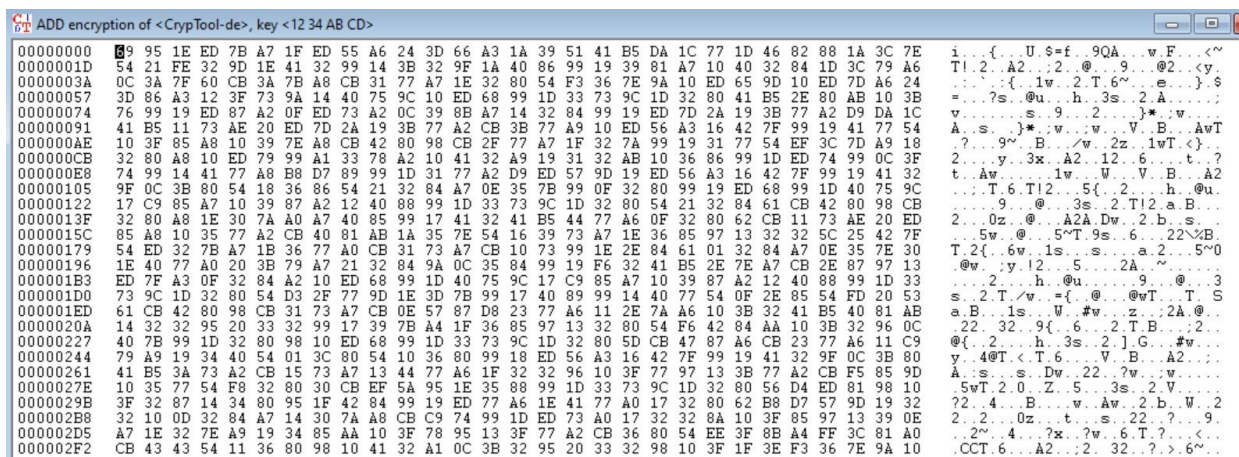
We can see the “E” occurred with more frequency. We can use the information later.

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

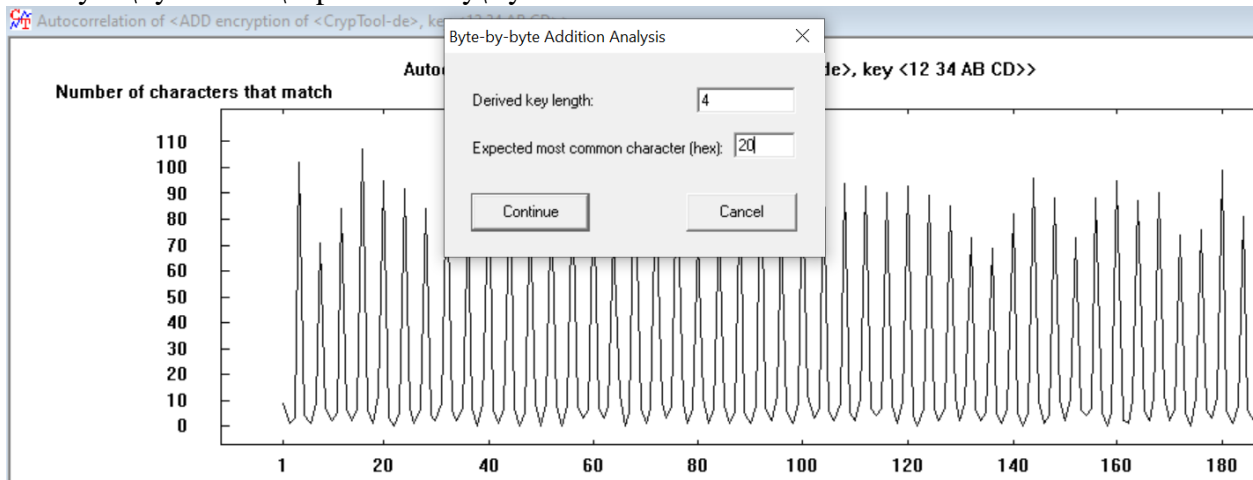
4. Enter 12 34 AB CD as the key and click Encrypt.



The encrypted message shows up:

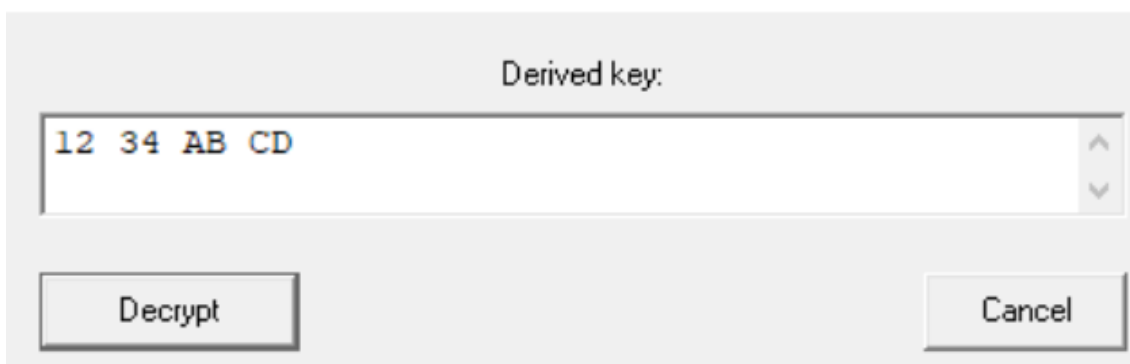


5. ciphertext only attack will be performed. Choose from menu “Analysis\Symmetric\Ciphertextonly\Byte Addition”.



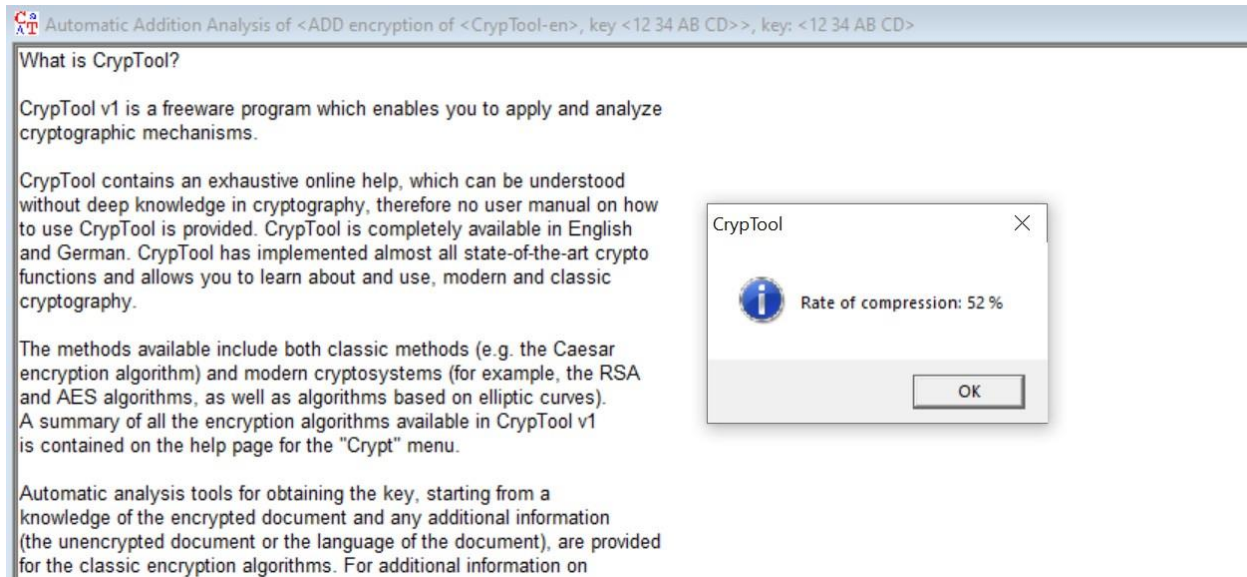
6. Click “Continue”, Cryptool has been able to find the key. The only information needed to do this was the fact that the character which occurred most frequently in the plaintext was the lower

Byte-by-byte Addition Analysis



case letter e.

7. Click the “Decrypt” button shows the plaintext.
8. To compress the document, we make startingexample-en.txt active again. And select “Indiv. Procedure\Tools\Compress\Zip”, the rate of compression is displayed.



Automatic Addition Analysis of <ADD encryption of <CrypTool-en>, key <12 34 AB CD>>, key: <12 34 AB CD>

What is CryptTool?

CrypTool v1 is a freeware program which enables you to apply and analyze cryptographic mechanisms.

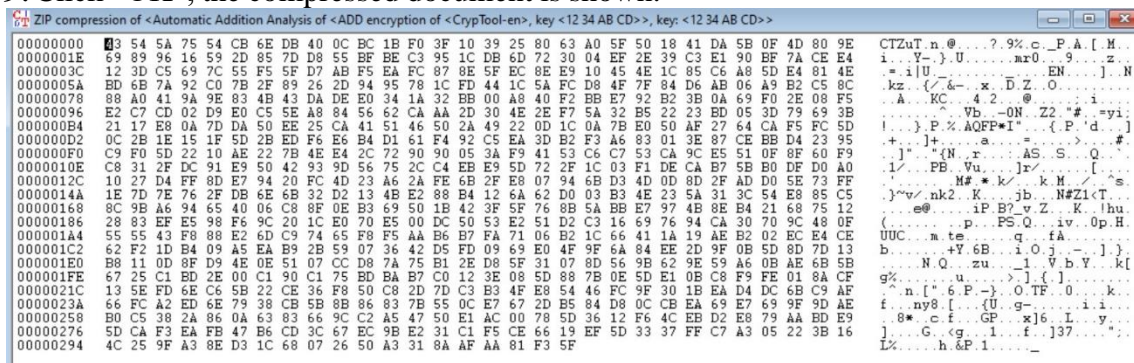
CrypTool contains an exhaustive online help, which can be understood without deep knowledge in cryptography, therefore no user manual on how to use CrypTool is provided. CrypTool is completely available in English and German. CrypTool has implemented almost all state-of-the-art crypto functions and allows you to learn about and use, modern and classic cryptography.

The methods available include both classic methods (e.g. the Caesar encryption algorithm) and modern cryptosystems (for example, the RSA and AES algorithms, as well as algorithms based on elliptic curves). A summary of all the encryption algorithms available in CrypTool v1 is contained on the help page for the "Crypt" menu.

Automatic analysis tools for obtaining the key, starting from a knowledge of the encrypted document and any additional information (the unencrypted document or the language of the document), are provided for the classic encryption algorithms. For additional information on

CrypTool
Rate of compression: 52 %
OK

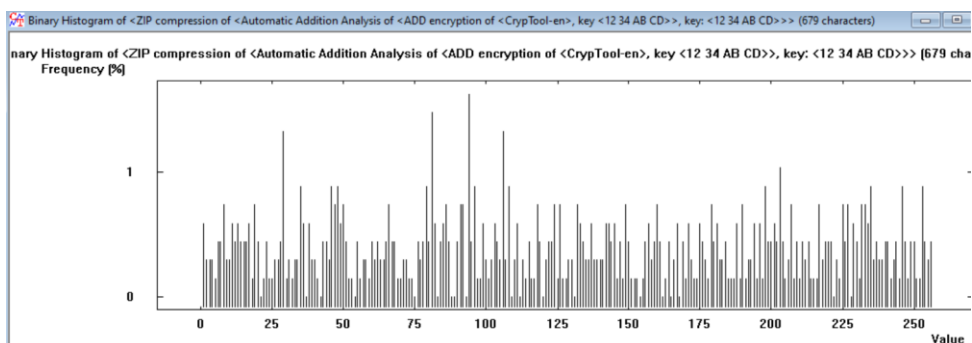
9. Click “OK”, the compressed document is shown.



ZIP compression of <Automatic Addition Analysis of <ADD encryption of <CrypTool-en>, key <12 34 AB CD>>, key: <12 34 AB CD>>

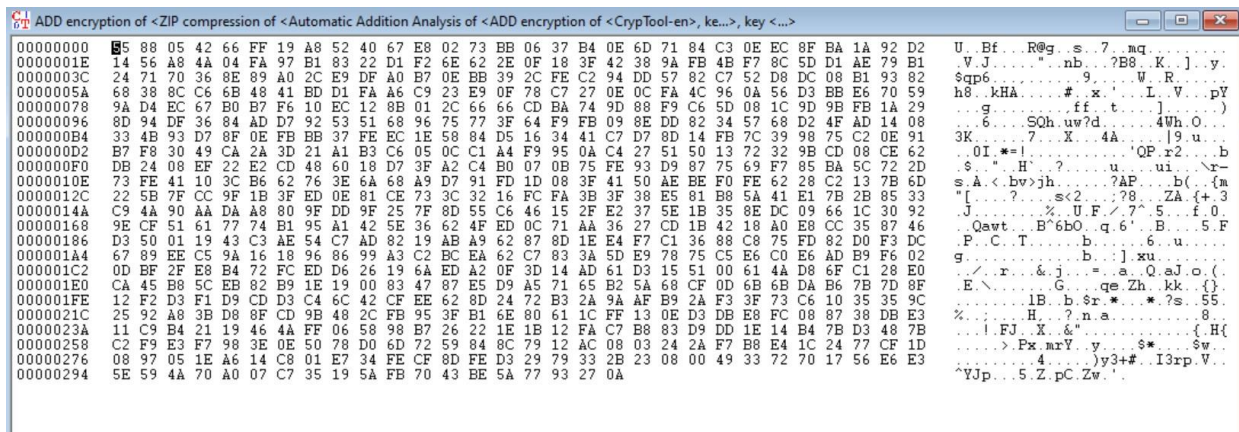
Offset	Hex	ASCII
00000000	54 5A 75 54 CB 6E DB 40 0C BC 1B F0 3F 10 39 25 80 63 A0 5F 50 18 41 DA 5B 0F 4D 80 9E	CTZuT.n.@...?.9% c_P.A.[.H...
00000001	69 89 96 16 59 2D 85 7D D8 55 BF BE C3 95 1C DB 6D 72 30 04 EF 2E 39 C3 E1 90 BF 7A CE E4	i...V-}.U...ar0...9...z...
00000002	12 3D C5 69 7C 55 F5 F5 D7 AB F5 EA FC 87 8E 5F EC 8E E9 10 45 4E 1C 85 C6 A8 5D E4 81 4E	= i U...}...EN...].N
00000003	BD 6B 7A 92 C0 7B 2F 89 26 2D 94 95 78 1C FD 44 1C 5A FC D8 4F 7F 84 D6 AB 06 A9 B2 C5 8C	kz.{/&-x.D.Z.O...
00000004	88 A0 41 9A 9E 83 4B 43 DA DE E0 34 1A 32 BB 00 A8 40 F2 BB E7 92 B2 3B 0A 69 F0 2E 08 F5	A...KC...4.2...@...i...
00000005	E2 C7 CD 02 D9 E0 C5 5E A8 84 56 62 CA AA 2D 30 4E 2E F7 5A 32 B5 22 23 BD 05 3D 79 69 3B	...Vb...-ON.ZZ.*#=yi...
00000006	21 17 E8 0A 7D DA 50 EE 25 CA 41 51 46 50 2A 49 22 0D 1C 0A 7B E0 50 AF 27 64 CA F5 FC 5D	!...}P.%AQFP*I...{P'd...]
00000007	0C 2B 1E 15 1F 5D 2B ED F6 E6 B4 D1 61 F4 92 C5 EA 3D B2 F3 A6 83 01 3E 87 CE EB D4 23 95]+...a...AS...Q...
00000008	C9 F0 5D 22 10 AE 22 7B 4E E4 2C 72 90 90 05 3A F9 41 53 C6 C7 53 CA 9C E5 51 0F 8F 60 F9	...}*(N.r...AS...S...Q...
00000009	C8 31 2F DC 91 E9 50 42 93 9D 56 75 2C C4 EB E9 5D 72 2F 1C 03 F1 DE CA B7 5B B0 DF D0 A0	1/...PB.Vu...}x/[...{...
00000010	10 27 D4 FF 8D E7 94 20 FC 4D 23 A6 2A FE 6B 2F E8 07 94 6B D3 4D 0D 8D 2F AD D0 5E 73 FF	M#.*k/k.k.M./s...
00000011	1E 7D 7E 76 2F DB 6E 6B 32 D2 13 4B E2 88 B4 12 6A 62 D0 03 B3 4E 23 5A 31 3C 54 E8 85 C5	}~v/nk2.K...jb...N#Zl<T...
00000012	8C 9B A6 94 65 40 06 C8 8F 0E B3 69 50 1B 42 3F 5F 76 8B 5A BB E7 97 4B 8E B4 21 68 75 12	e@...iP.B?_v.Z...K...!hu...
00000013	28 83 EF E5 98 F6 9C 20 1C E0 70 E5 00 DC 50 53 E2 51 D2 C3 16 69 76 94 CA 30 70 9C 48 0F	(...e@...p...FS.Q...iv...0p.H...
00000014	55 55 43 F9 88 E2 6D C9 74 65 F8 F5 AA B6 B7 FA 71 06 B2 1C 66 41 1A 19 AE B2 02 EC E4 CE	UUC...a...te...q...fA...
00000015	62 F2 1D B4 09 A5 EA B9 2B 59 07 36 42 D5 FD 09 69 E0 4F 9F 6A 84 EE 2D 9F 0B 5D 8D 7D 13	b...+v6B...iOj...-...]}...
00000016	B8 11 0D 8F D9 4E 0E 51 07 CC D8 7A 75 B1 2E D8 5F 31 07 8D 56 9B 62 9E 59 A6 0B AE 6B 5B	N.Q...zu...l.Vb.V...k[...
00000017	67 25 C1 BD 2E 00 C1 90 C1 75 BD BA B7 C0 12 3E 08 5D 88 7B 0E 5D E1 0B C8 F9 FE 01 8A CF	g%...u...>...l{...}
00000018	13 5E FD 6E C6 5B 22 CE 36 F8 50 C8 2D 7D C3 B3 4F E8 54 46 FC 9F 30 1B EA D4 DC 6B C9 AF	n["6.P-).O.TF.0...k...
00000019	66 FC A2 ED 6E 79 38 CB 5B 8B 86 83 7B 55 0C E7 67 2D B5 84 D8 0C CB EA 69 E7 69 9F 9D AE	f...ny8[...]U...g...i...i...
00000020	B0 C5 38 2A 86 0A 63 83 66 9C C2 A5 47 50 E1 AC 00 78 5D 36 12 F6 4C EB D2 E8 79 AA BD E9	8*c.f...GP...x]6...L...y...
00000021	5D CA F3 EA FB 47 B8 CD 3C 67 EC 9B E2 31 C1 F5 CE 5B 19 EF 5D 33 37 FF C7 A3 05 22 3B 16]...G...g...l...f...j37...
00000022	4C 25 9F A3 8E D3 1C 68 07 26 50 A3 31 8A AF AA 81 F3 5F	LZ...h&P.1.....

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 unencrypted document. The characters are much more evenly



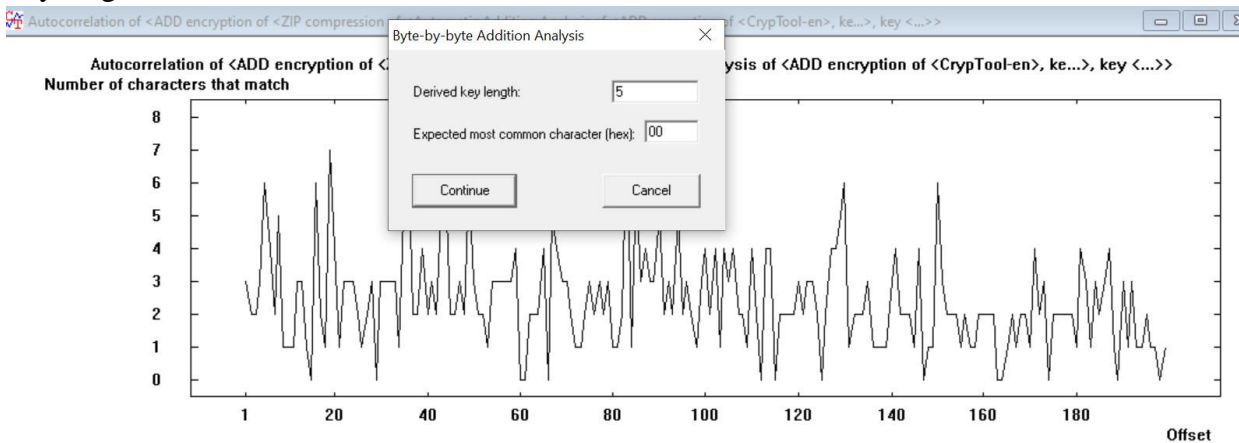
distributed than in the unencrypted document.

11. Now encrypt as the same as the previous, use the key 12 34 AB CD and click on Encrypt.

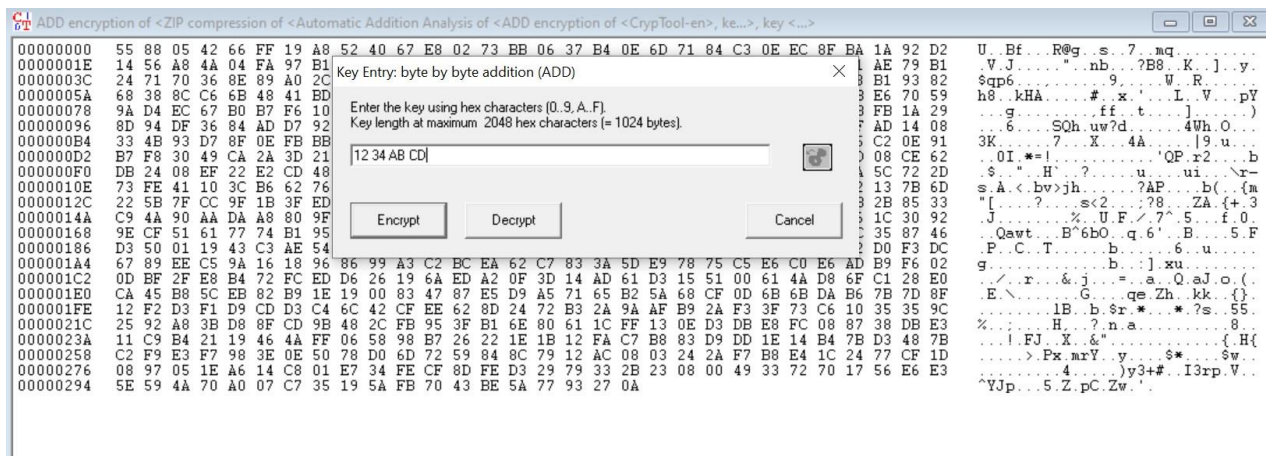


12. Now Analyze same as the previous we did, it is different now.

Key length is returned incorrect here as 5.

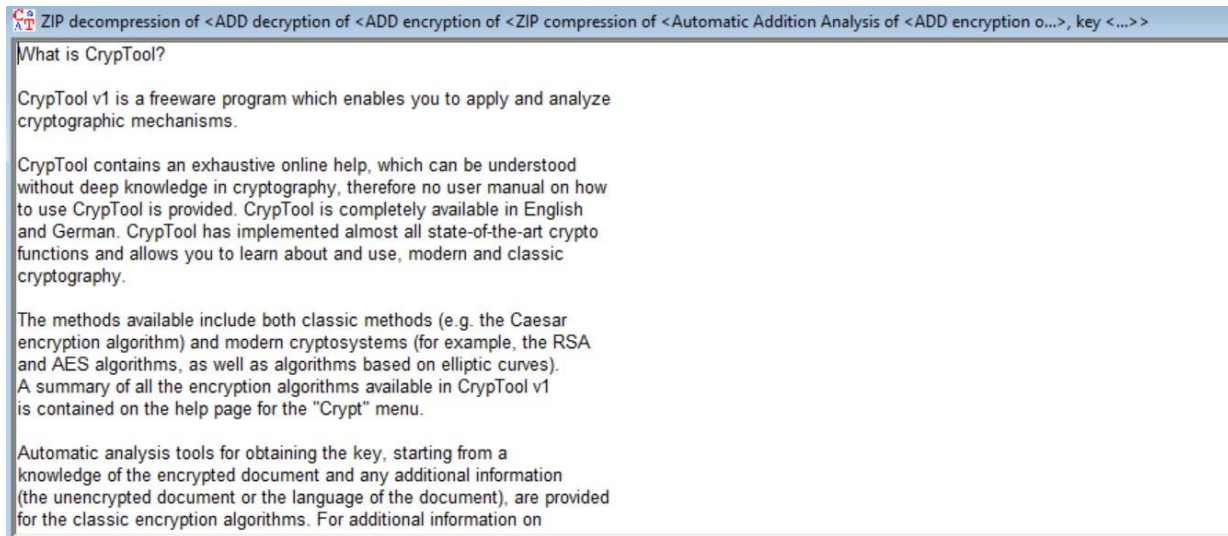


13. Since it returned the wrong key length, we will decrypt and unzip.



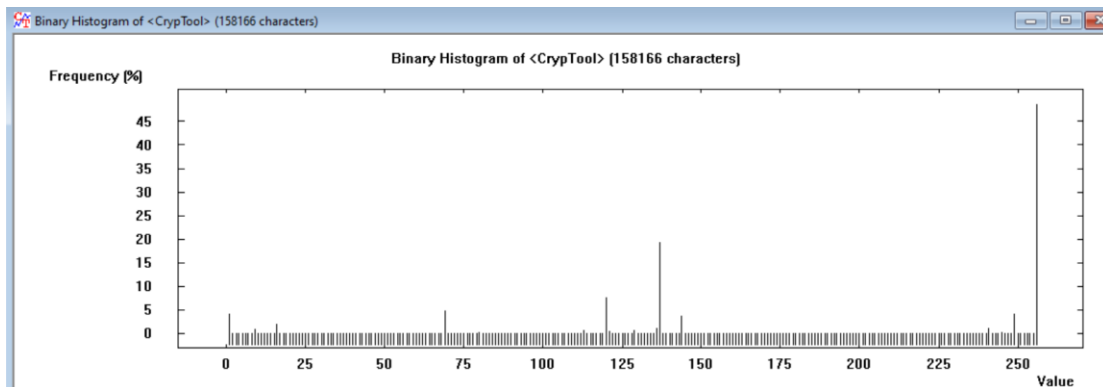
Enter 12 34 AB CD as the key and click Decrypt.

14. Now Unzip it, Choose from menu “Indiv. Procedure\Tools\Compress\UnZip”, and the original text is displayed.



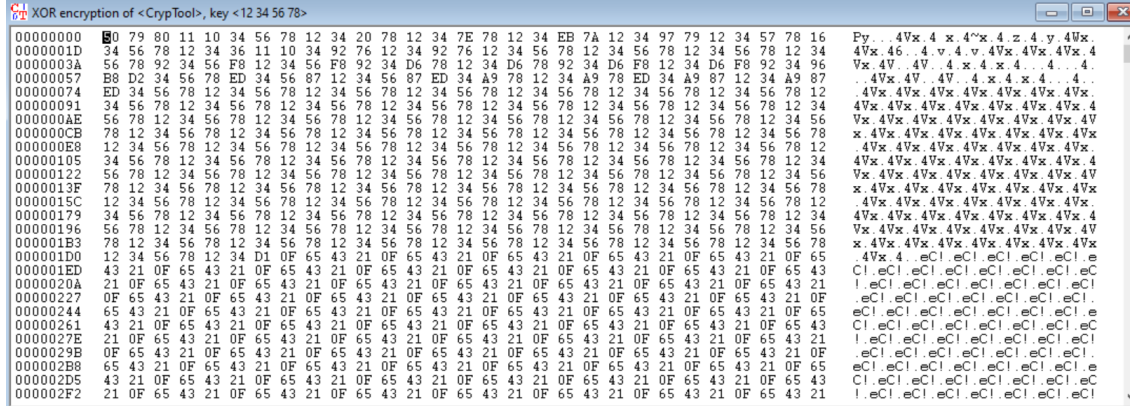
Lab-Binary XoR:

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”

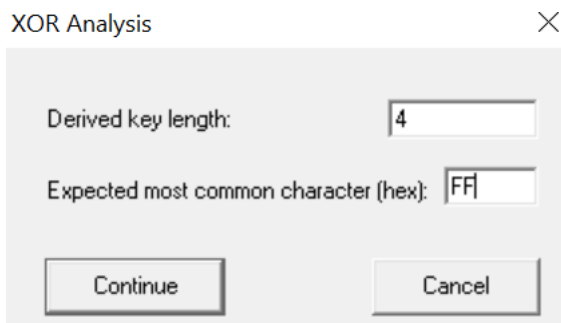


The most frequent occurrence is 255 and its value is FF.

3. click “Encrypt\Decrypt\Symmetric\XOR” from the menu. Then enter 12 34 56 78 as the key and Click “Encrypt”

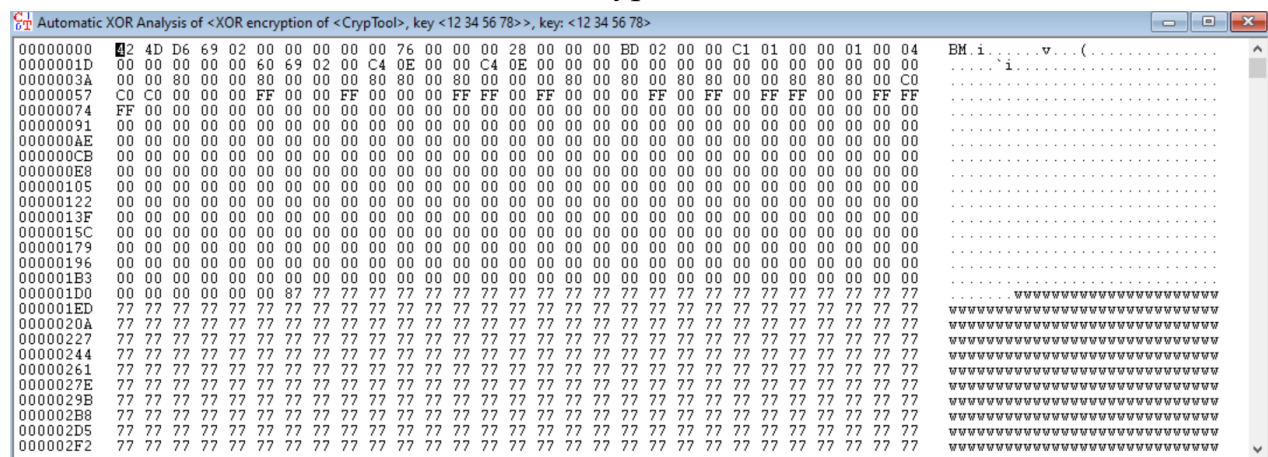


4. We will perform the cipher-text only attack. Select “Analysis\Symmetric Encryption\CiphertextOnly\XOR”. The autocorrelation is calculated and displayed. We are told that the key length is calculated to be 4. As we have seen in step 2, the most common character is



FF. This we enter in the Expected most common character field.

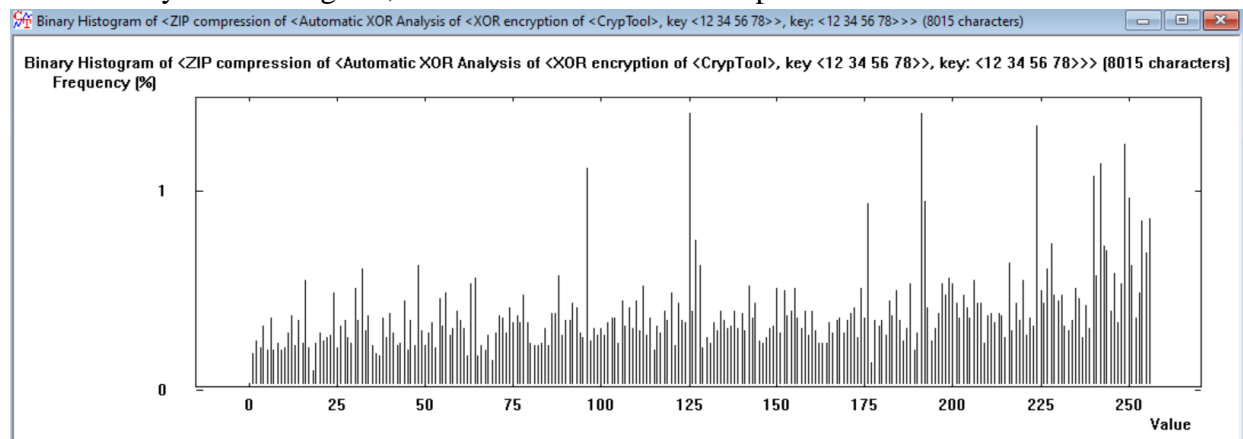
5. Click “continue” and then Click “Decrypt”.



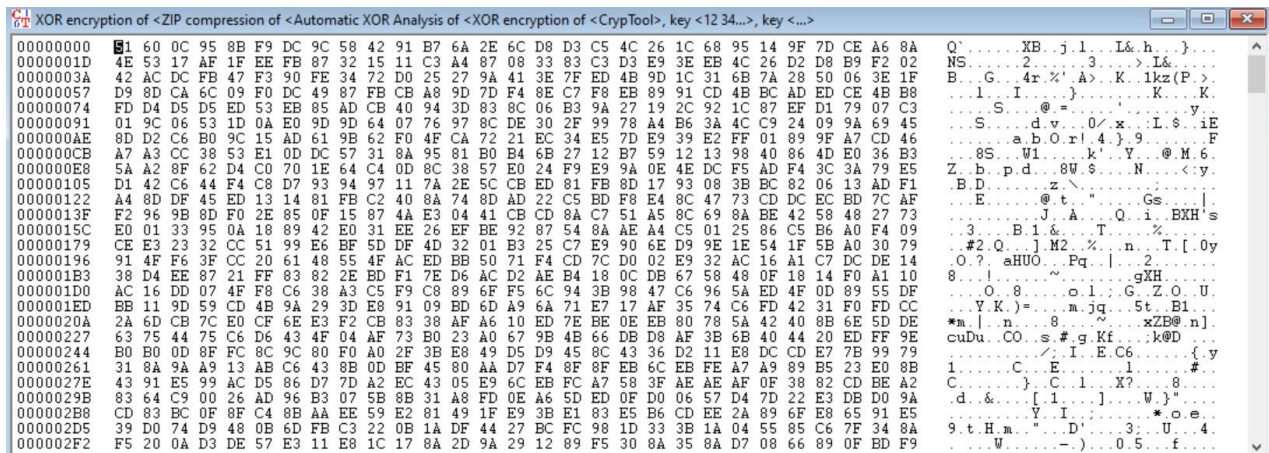
6. Now we have to zip it before encryption, by clicking “Indiv. Procedure\Tools\Compress\Zip”.



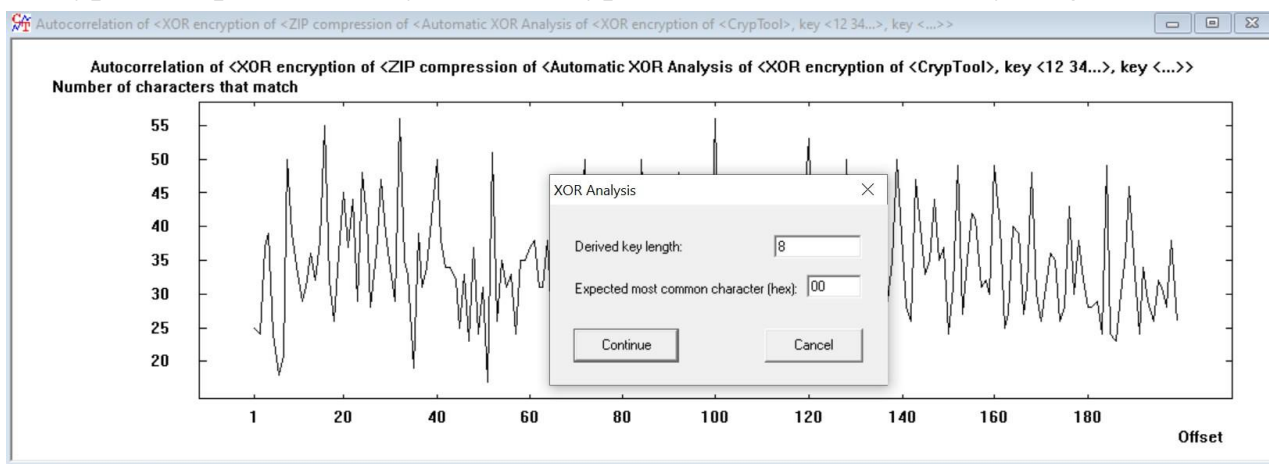
7. Now analyze the histogram, it will be different from the previous.



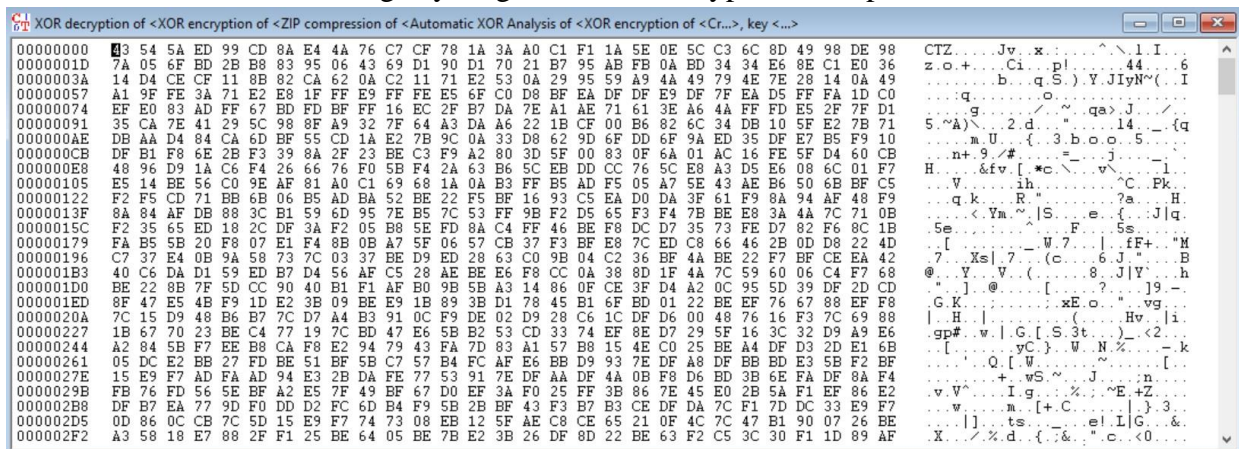
8. Encrypt the compressed document by selecting “Encrypt\Decrypt\Symmetric/XOR” from menu and use 12 34 56 78 as the key.



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



10. Since it returned the wrong key length, we will decrypt and unzip.



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

11. Now Unzip it, Choose from menu “Indiv. Procedure\Tools\Compress\UnZip”, and the original text is displayed.

