Text 1.

It is homogeneous text which consist of 1500 characters of letter “v”

Text 2

Medium diversified text consisting of the phrase “Once You Question Your Own Belief, It's Over” Repeated 1500 times

Text 3

Highly diversified text id lorem ipsum text with approximately 1500 characters

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Maecenas feugiat risus eu justo consectetur, eget ultrices ante eleifend. Vestibulum scelerisque elit id tortor scelerisque, sit amet posuere purus aliquet. Nullam feugiat justo eu dui viverra, sit amet scelerisque augue volutpat. Sed et libero non ligula tincidunt interdum. Curabitur eget augue et sapien aliquet vehicula. Fusce ac magna non arcu ullamcorper vulputate. In at metus et tortor eleifend euismod. Sed nec nunc nec massa pharetra lacinia. Nunc eu purus consectetur, iaculis justo id, dapibus nulla. Proin a sapien at quam sollicitudin pellentesque. Sed eu nisl in risus bibendum volutpat. Aenean tristique mauris ac quam aliquam, a facilisis nulla auctor. Vestibulum volutpat libero a justo congue, eu scelerisque eros pharetra. Nullam lacinia urna in libero iaculis, sit amet euismod urna euismod.

Fusce volutpat tortor ut tortor volutpat, eget consectetur sem eleifend. Sed at purus id odio condimentum tristique id a neque. Curabitur sit amet mauris vel ante semper sagittis. Vestibulum vel sapien ut arcu semper elementum nec vel elit. Phasellus ultrices justo at felis fringilla, ut tincidunt justo rhoncus. Suspendisse ultrices arcu vel libero lacinia, et gravida sem feugiat. Maecenas tincidunt justo a lacinia blandit. Nullam sit amet lectus ut arcu malesuada tincidunt. Vivamus euismod eros ut augue vehicula, eget dictum risus venenatis. Integer eu sapien eget nunc mattis congue. Nullam sed metus eget ipsum auctor sollicitudin. Sed ut bibendum est. Nullam laoreet lorem ac sapien sodales, vel cursus quam euismod. Vivamus tincidunt lectus in est malesuada, at fermentum sapien pellentesque.

Pellentesque quis ligula eu nulla dignissim varius ac eu purus. Quisque nec turpis eget ex pellentesque gravida. Ut non tellus sit amet sapien dapibus dictum. Aliquam erat volutpat.

For analysis I have chosen IDEA,DES and AES

IDEA key: B936F332FC3F23B0F83F3BFC391283FC

DES(ECB) key: 236985F410B62246

AES(CBC) 128key: B936F332FC3F23B0F83F3BFC391283FC

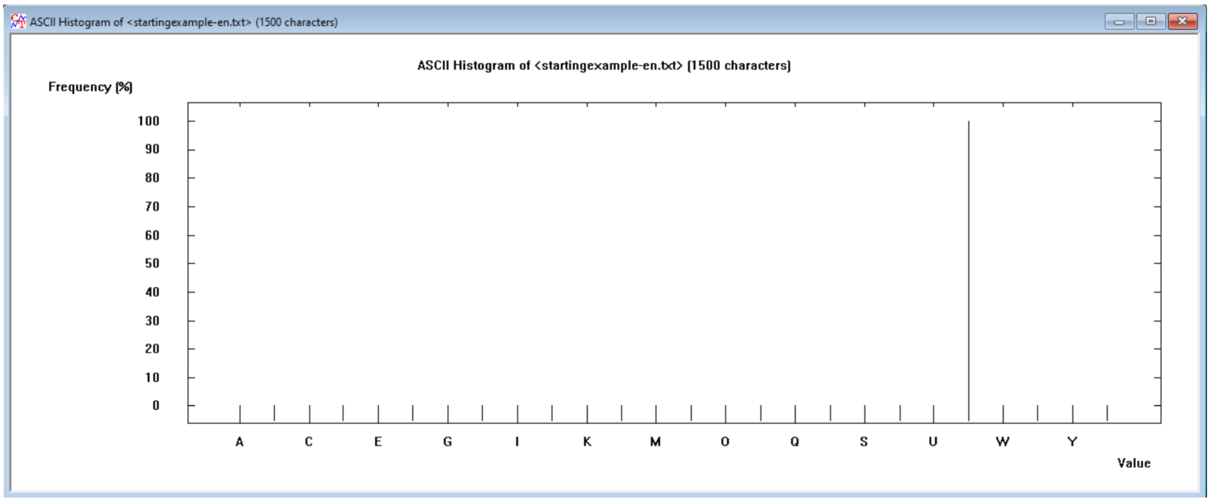
AES(CBC) 192key: 9137F139F139C130C13097FFC13471340C311397340349C3

AES(CBC) 256key: 1348F39F7319F13F1303931F13D1D01A781ADFEEF9CC01265C12394CAF013081

Scale out of 4.7

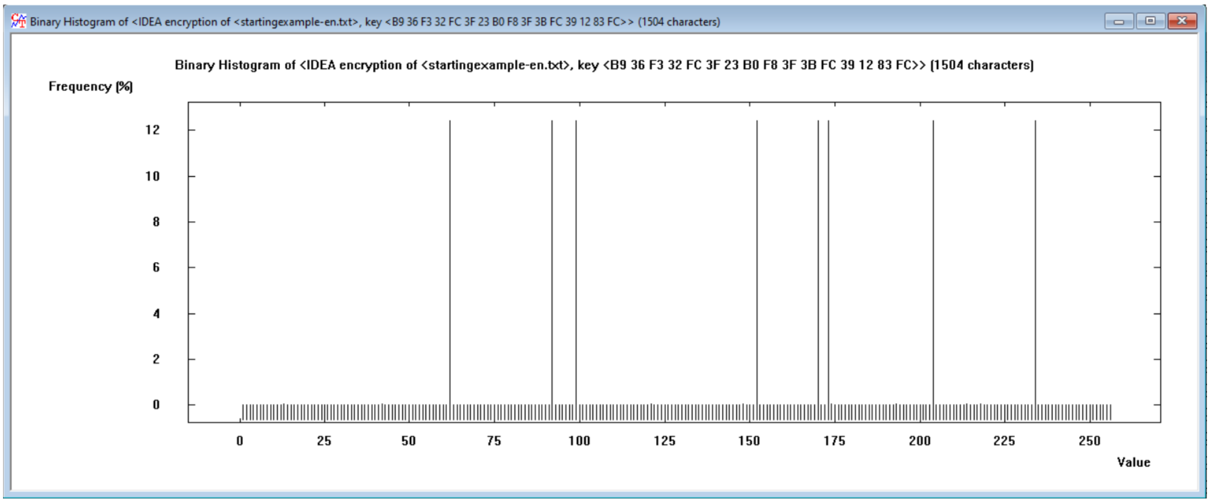
Entropy comparison			
Algorithm	Key Length(bits)	Plaintext	Ciphertext
IDEA	128	0,00	1.786
		3.72	4.5375
		3.96	4.64125
DES(ECB)	64	0,00	1.786
		3.72	4.00675
		3.96	4.6295
AES(CBC)	128	0,00	4.6295
		3.72	4.694125
		3.96	4.6295
	192	0,00	4.623625
		3.72	4.694125
		3.96	4.647125
	256	0,00	4.61775
		3.72	4.694125
		3.96	4.694125

Homogeneous text consisting of only “v” letter:



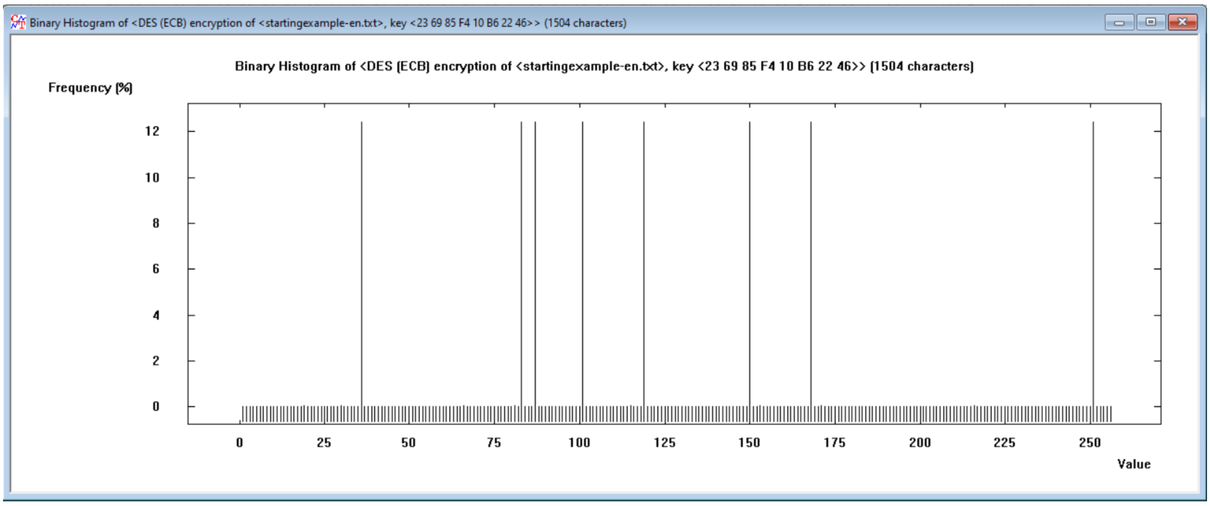
ASCII Histogram of <startingexample-en.txt> (1500 characters)

ASCII Histogram of <startingexample-en.txt> (1500 characters)



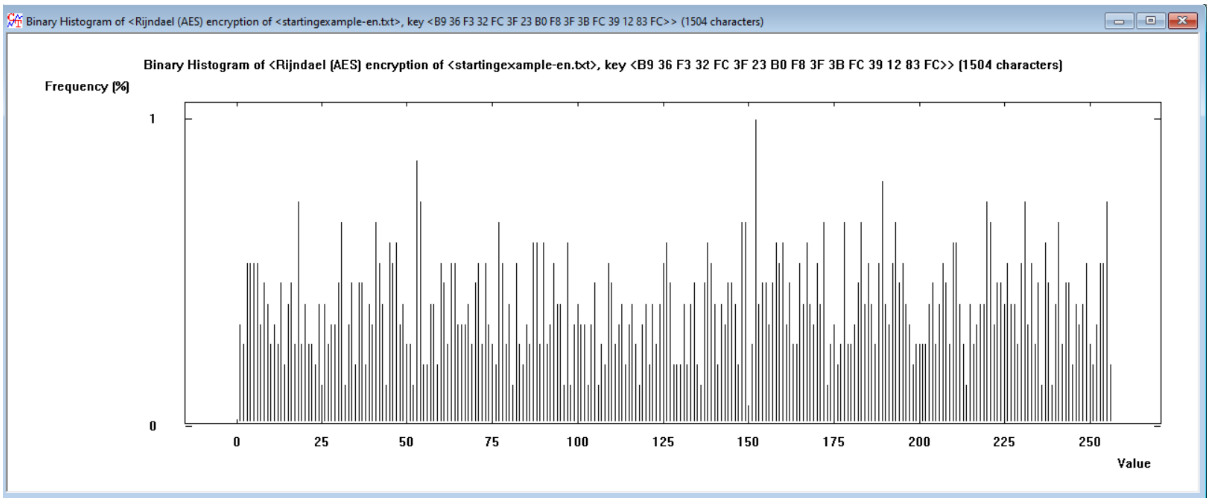
Binary Histogram of <IDEA encryption of <startingexample-en.txt>, key <B9 36 F3 32 FC 3F 23 B0 F8 3F 3B FC 39 12 83 FC>> (1504 characters)

Binary Histogram of <IDEA encryption of <startingexample-en.txt>, key <B9 36 F3 32 FC 3F 23 B0 F8 3F 3B FC 39 12 83 FC>> (1504 characters)



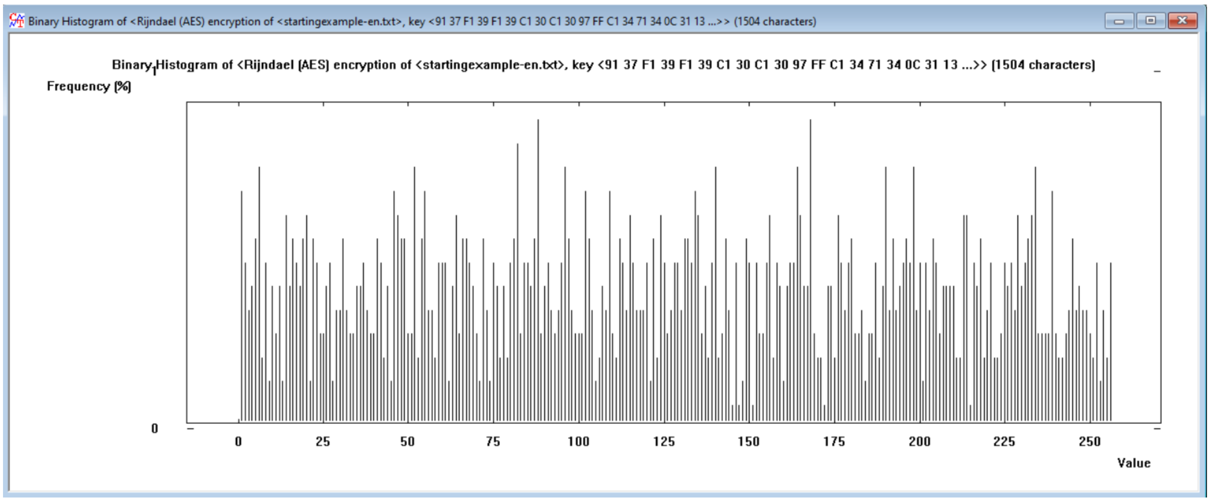
Binary Histogram of <DES (ECB) encryption of <startingexample-en.txt>, key <23 69 85 F4 10 B6 22 46>> (1504 characters)

Binary Histogram of <DES (ECB) encryption of <startingexample-en.txt>, key <23 69 85 F4 10 B6 22 46>> (1504 characters)



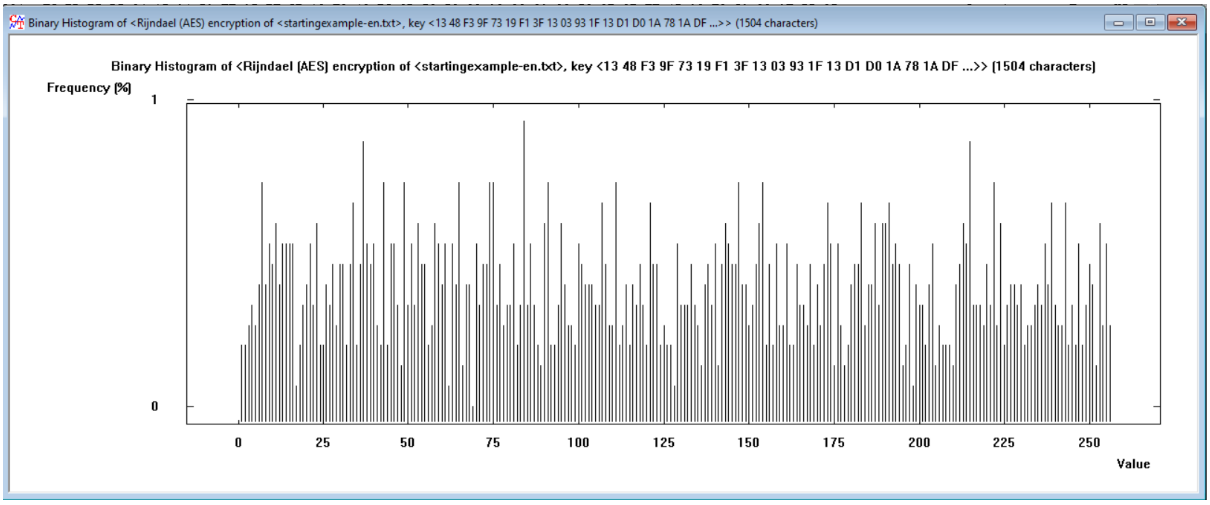
Binary Histogram of <Rijndael (AES) encryption of <startingexample-en.txt>, key <B9 36 F3 32 FC 3F 23 B0 F8 3F 3B FC 39 12 83 FC>> (1504 characters)

Binary Histogram of <Rijndael (AES) encryption of <startingexample-en.txt>, key <B9 36 F3 32 FC 3F 23 B0 F8 3F 3B FC 39 12 83 FC>> (1504 characters)



Binary Histogram of <Rijndael (AES) encryption of <startingexample-en.txt>, key <91 37 F1 39 F1 39 C1 30 C1 30 97 FF C1 34 71 34 0C 31 13 ...>> (1504 characters)

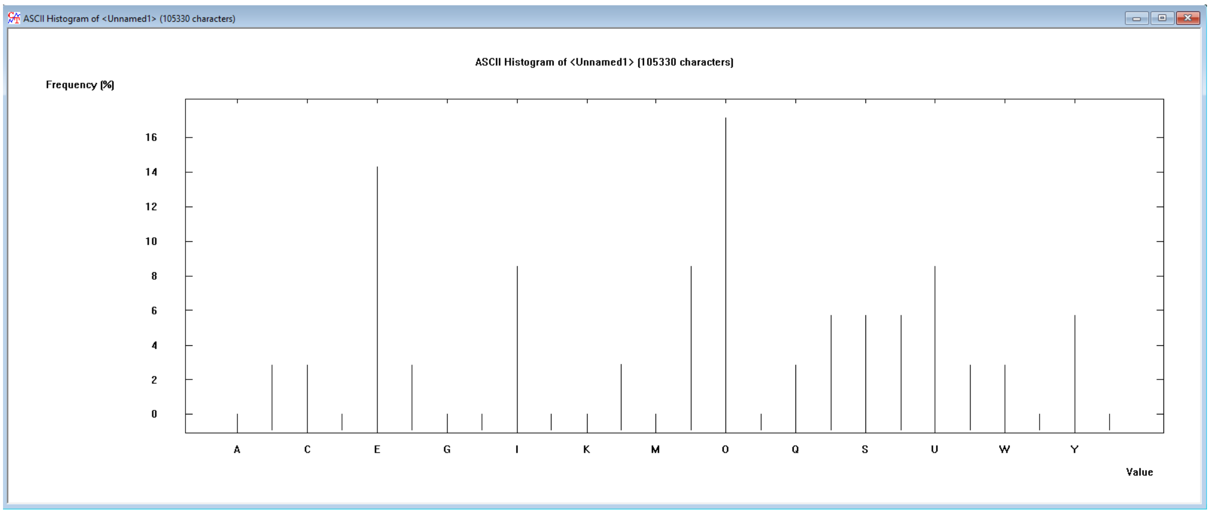
Binary Histogram of <Rijndael (AES) encryption of <startingexample-en.txt>, key <91 37 F1 39 F1 39 C1 30 C1 30 97 FF C1 34 71 34 0C 31 13 ...>> (1504 characters)



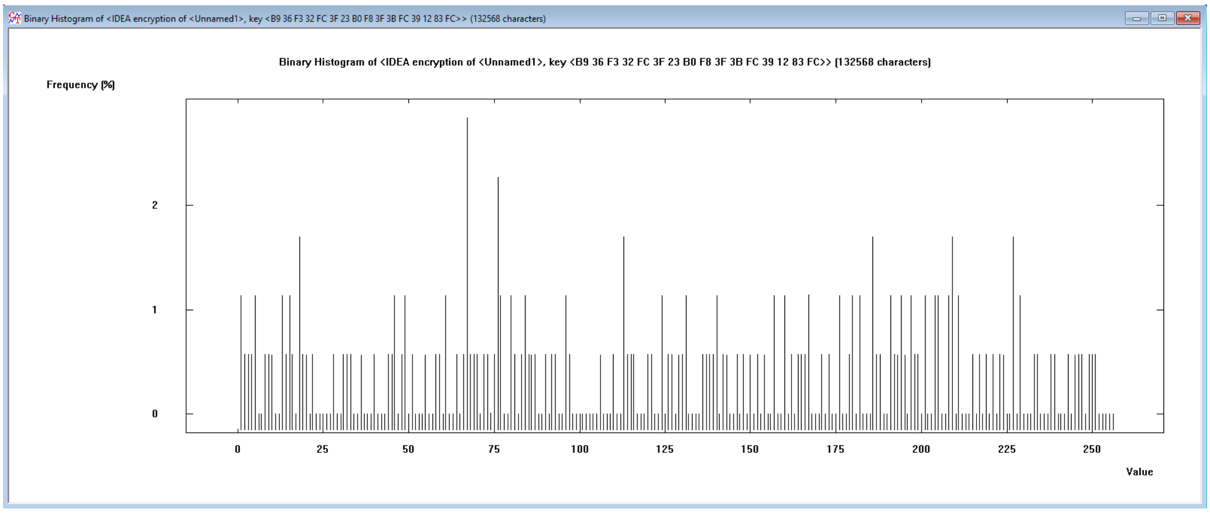
Binary Histogram of <Rijndael (AES) encryption of <startingexample-en.txt>, key <13 48 F3 9F 73 19 F1 3F 13 03 93 1F 13 D1 D0 1A 78 1A DF ...>> (1504 characters)

Binary Histogram of <Rijndael (AES) encryption of <startingexample-en.txt>, key <13 48 F3 9F 73 19 F1 3F 13 03 93 1F 13 D1 D0 1A 78 1A DF ...>> (1504 characters)

Medium-diversified text:

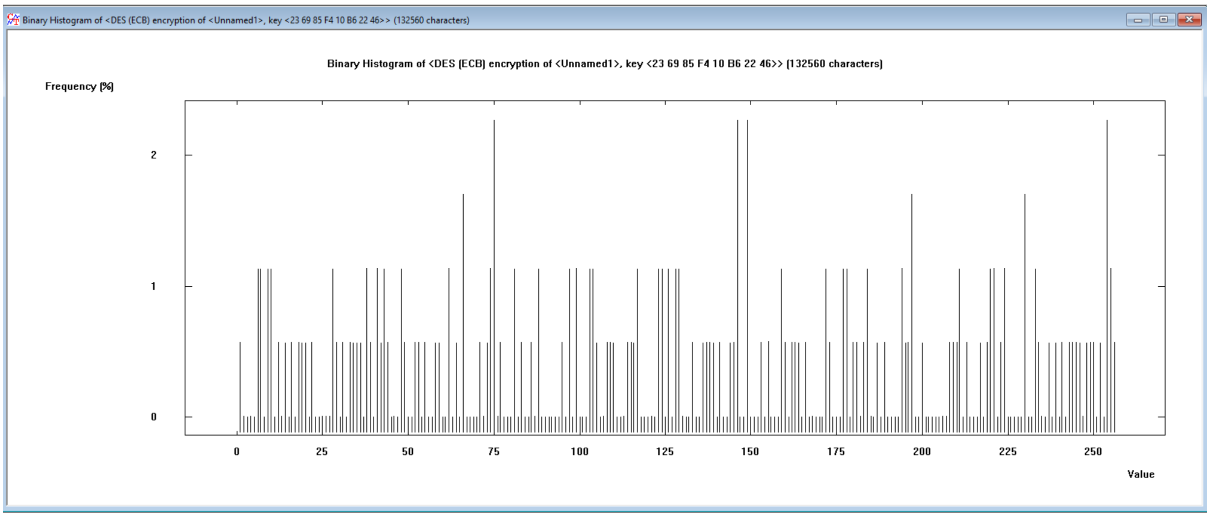


ASCII Histogram of <Unnamed1> (105330 characters)



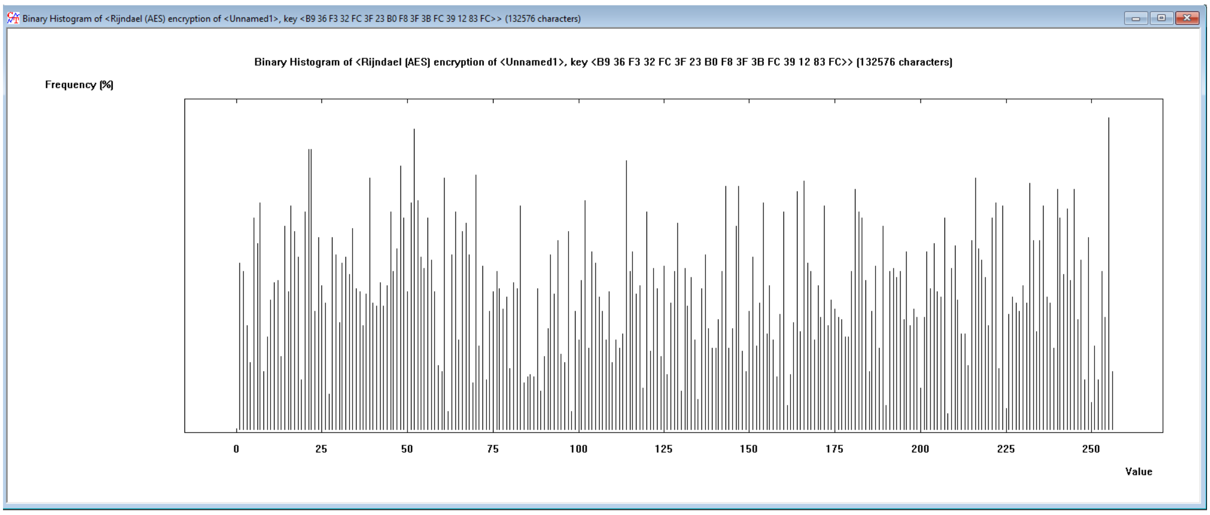
Binary Histogram of <IDEA encryption of <Unnamed1>, key <B9 36 F3 32 FC 3F 23 B0 F8 3F 3B FC 39 12 83 FC>> (132568 characters)

Binary Histogram of <IDEA encryption of <Unnamed1>, key <B9 36 F3 32 FC 3F 23 B0 F8 3F 3B FC 39 12 83 FC>> (132568 characters)
Frequency (%)
2
1
0
0
25
50
75
100
125
150
175
200
225
250
Value



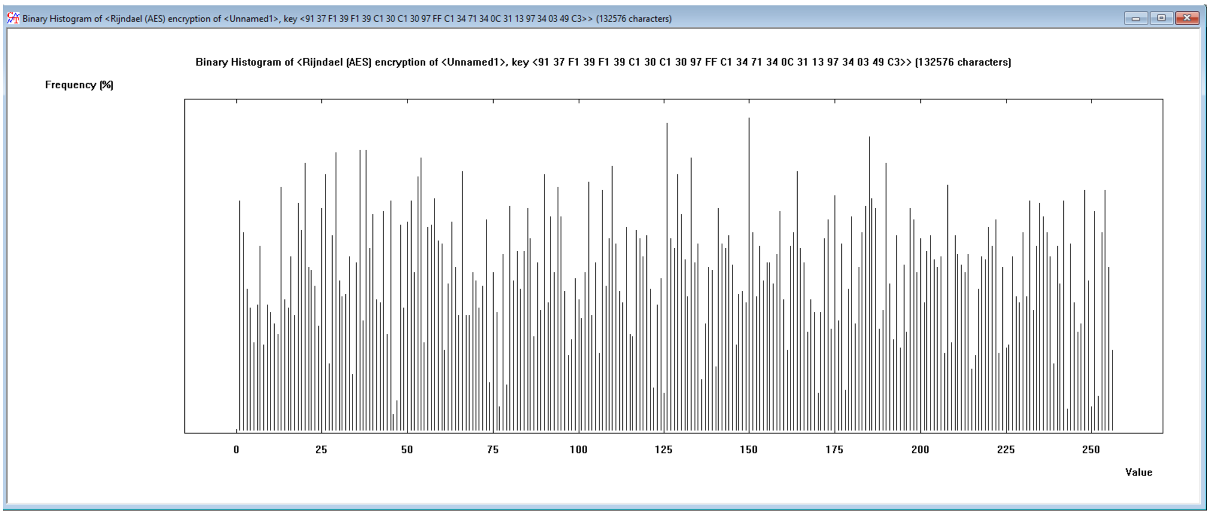
Binary Histogram of <DES (ECB) encryption of <Unnamed1>, key <23 69 85 F4 10 B6 22 46>> (132560 characters)

Binary Histogram of <DES (ECB) encryption of <Unnamed1>, key <23 69 85 F4 10 B6 22 46>> (132560 characters)
Frequency (%)
2
1
0
0
25
50
75
100
125
150
175
200
225
250
Value



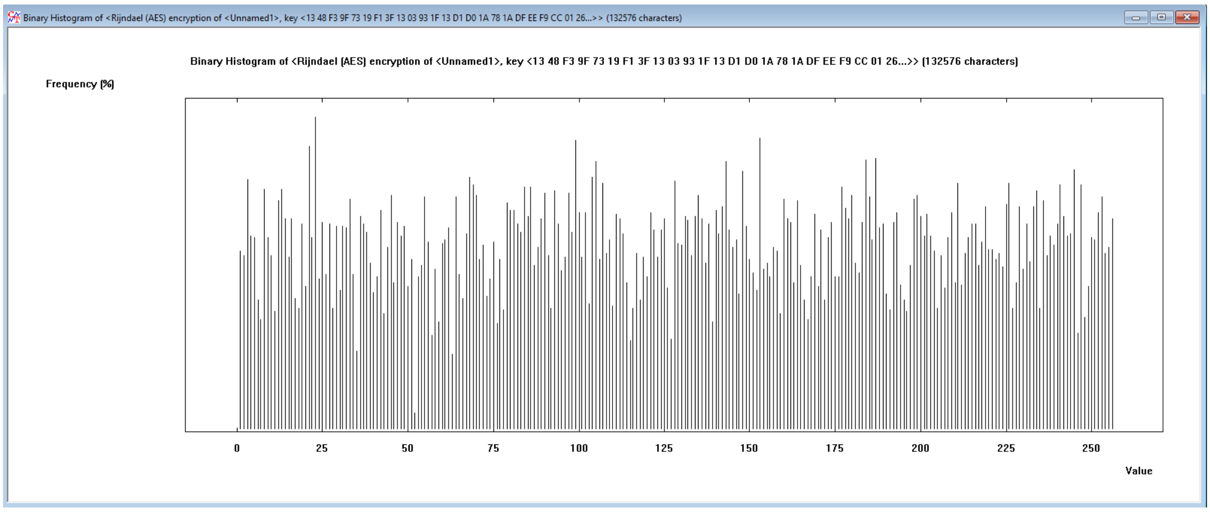
Binary Histogram of <Rijndael (AES) encryption of <Unnamed1>, key <B9 36 F3 32 FC 3F 23 B0 F8 3F 3B FC 39 12 83 FC>> (132576 characters)

Binary Histogram of <Rijndael (AES) encryption of <Unnamed1>, key <B9 36 F3 32 FC 3F 23 B0 F8 3F 3B FC 39 12 83 FC>> (132576 characters)



Binary Histogram of <Rijndael (AES) encryption of <Unnamed1>, key <91 37 F1 39 F1 39 C1 30 C1 30 97 FF C1 34 71 34 0C 31 13 97 34 03 49 C3>> (132576 characters)

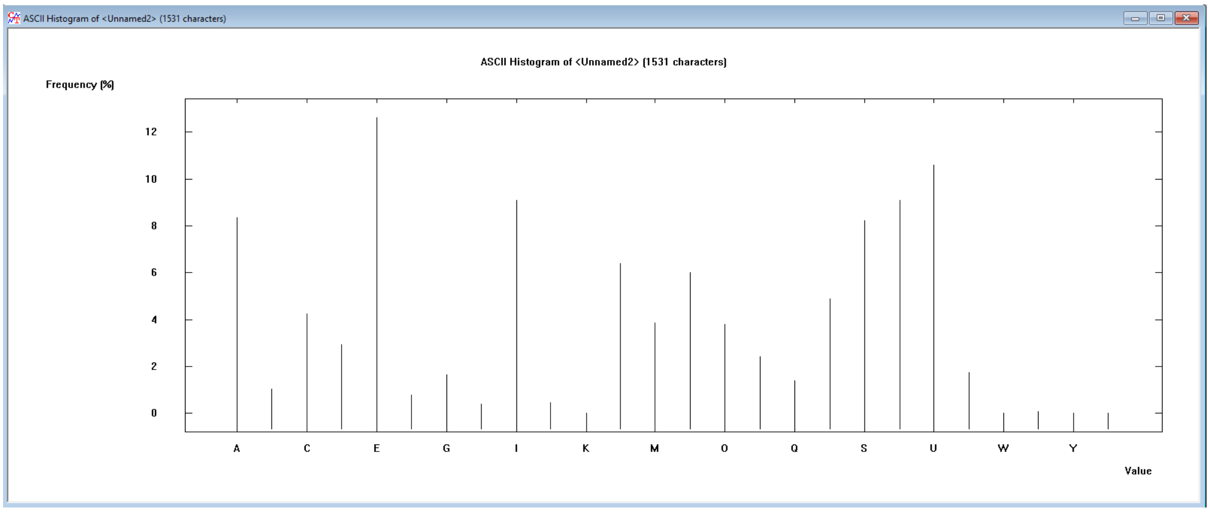
Binary Histogram of <Rijndael (AES) encryption of <Unnamed1>, key <91 37 F1 39 F1 39 C1 30 C1 30 97 FF C1 34 71 34 0C 31 13 97 34 03 49 C3>> (132576 characters)



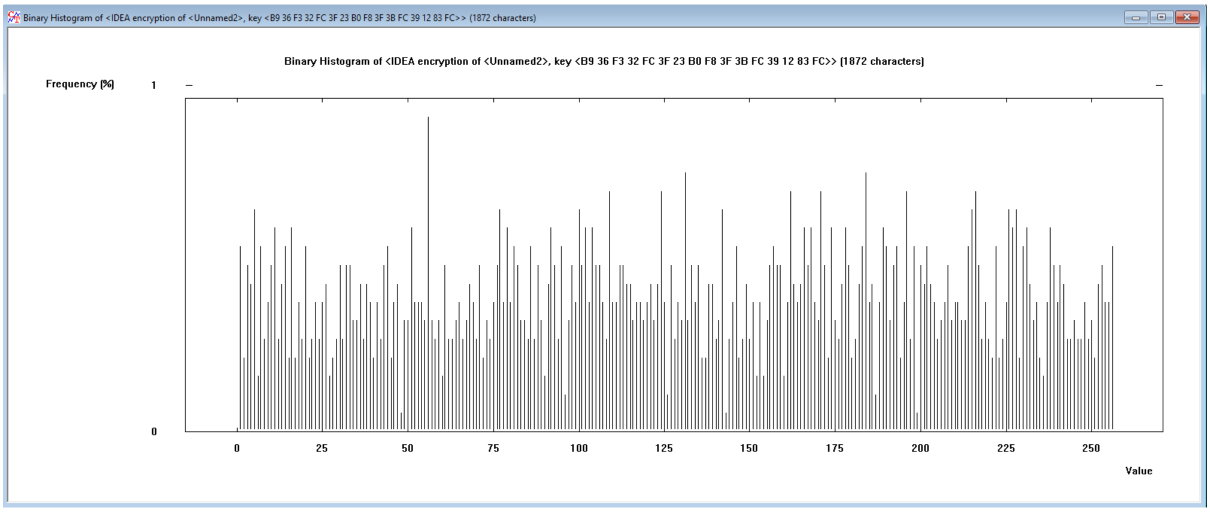
Binary Histogram of <Rijndael (AES) encryption of <Unnamed1>, key <13 48 F3 9F 73 19 F1 3F 13 03 93 1F 13 D1 D0 1A 78 1A DF EE F9 CC 01 26...>> (132576 characters)

Binary Histogram of <Rijndael (AES) encryption of <Unnamed1>, key <13 48 F3 9F 73 19 F1 3F 13 03 93 1F 13 D1 D0 1A 78 1A DF EE F9 CC 01 26...>> (132576 characters)

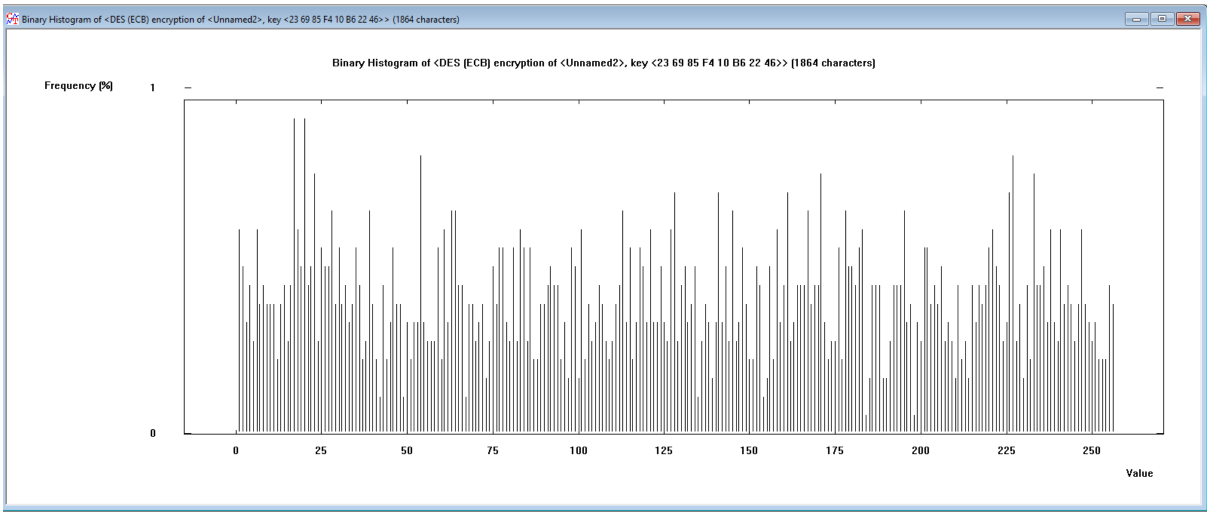
Highly-diversified text:


ASCII Histogram of <Unnamed2> (1531 characters)

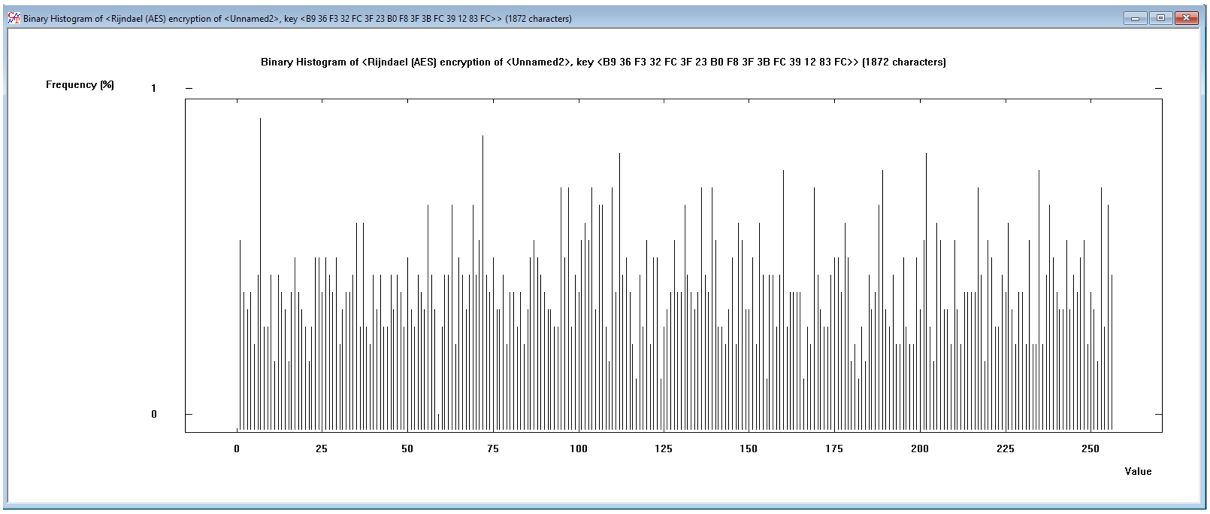
ASCII Histogram of <Unnamed2> (1531 characters)


Binary Histogram of <IDEA encryption of <Unnamed2>, key <B9 36 F3 32 FC 3F 23 B0 F8 3F 3B FC 39 12 83 FC>> (1872 characters)

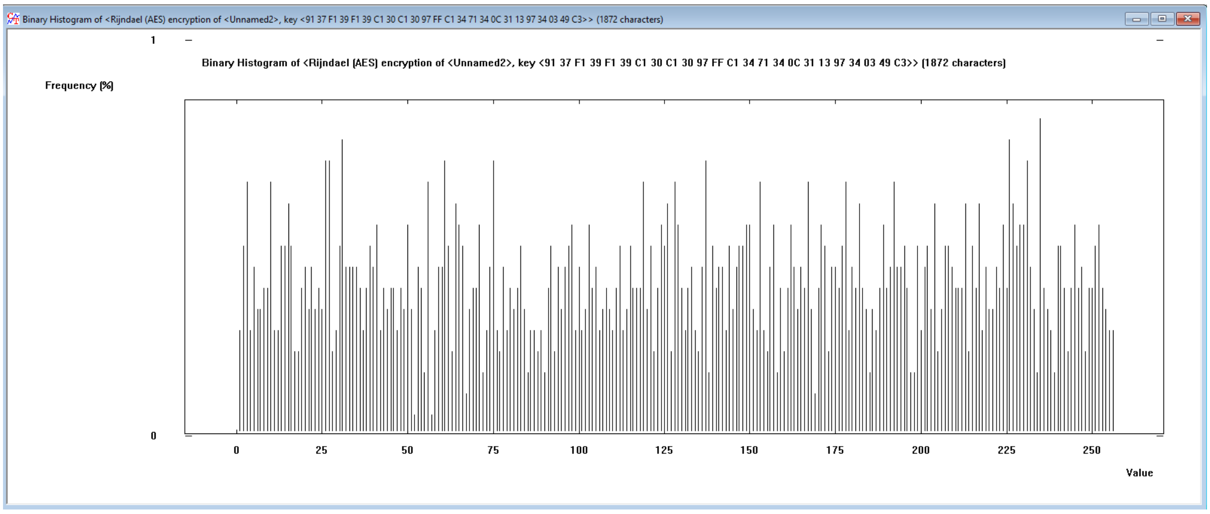
Binary Histogram of <IDEA encryption of <Unnamed2>, key <B9 36 F3 32 FC 3F 23 B0 F8 3F 3B FC 39 12 83 FC>> (1872 characters)


Binary Histogram of <DES (ECB) encryption of <Unnamed2>, key <23 69 85 F4 10 B6 22 46>> (1864 characters)

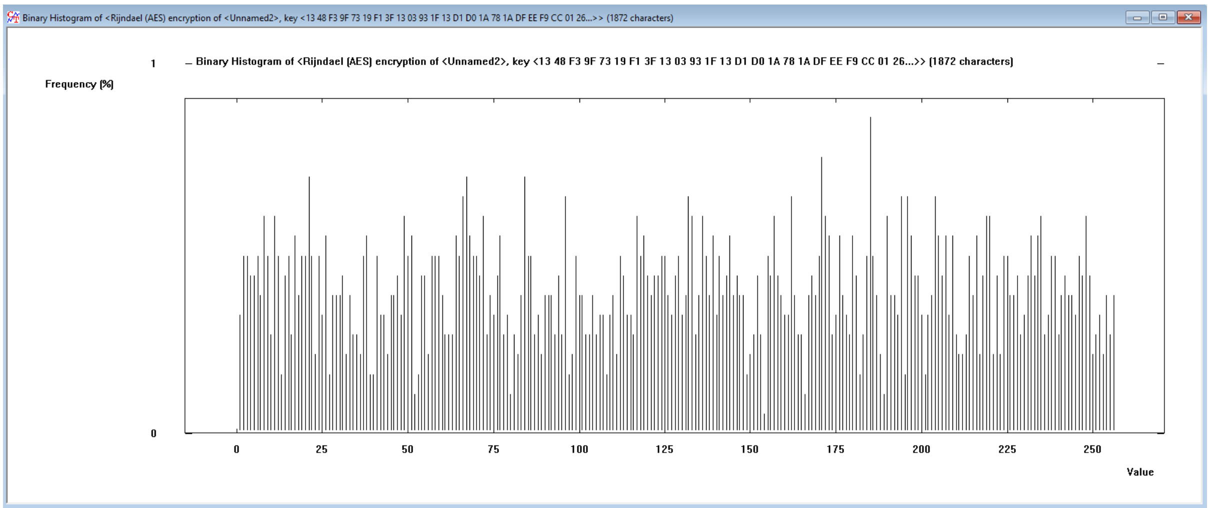
Binary Histogram of <DES (ECB) encryption of <Unnamed2>, key <23 69 85 F4 10 B6 22 46>> (1864 characters)



Binary Histogram of <Rijndael (AES) encryption of <Unnamed2>, key <B9 36 F3 32 FC 3F 23 B0 F8 3F 3B FC 39 12 83 FC>> (1872 characters)



Binary Histogram of <Rijndael (AES) encryption of <Unnamed2>, key <91 37 F1 39 F1 39 C1 30 C1 30 97 FF C1 34 71 34 0C 31 13 97 34 03 49 C3>> (1872 characters)



Binary Histogram of <Rijndael (AES) encryption of <Unnamed2>, key <13 48 F3 9F 73 19 F1 3F 13 03 93 1F 13 D1 D0 1A 78 1A DF EE F9 CC 01 26...>> (1872 characters)

TASK 1.3

AES, the Advanced Encryption Standard, is the trusted standard algorithm used by the United States government and other organizations. It offers highly efficient encryption in 128-bit form, but also provides the flexibility to use larger key sizes of 192 and 256 bits for the most demanding encryption purposes. AES operates with a fixed block size of 128 bits, which is one of its distinguishing features. This block size is integral to its effectiveness in securing data, and it is widely considered invulnerable to all attacks except for brute force. Regardless, many internet security experts believe that AES, with its robust block size, will eventually be regarded as the go-to standard for encrypting data in the private sector.

RSA is a widely-used public-key encryption algorithm and is considered the standard for securing data transmitted over the internet. It is also commonly utilized in encryption programs such as PGP and GPG. Unlike symmetric algorithms like Triple DES, RSA is an asymmetric encryption algorithm, meaning it relies on a pair of keys. Users possess a public key for encrypting messages and a private key for decrypting them. When RSA encryption is employed, it generates a ciphertext that appears as a complex jumble of characters, making it computationally demanding for attackers to decipher.

The strength and security of RSA are determined by the key size. The key size is measured in bits and affects the algorithm's effectiveness in protecting data. In practice, commonly recommended key sizes for RSA encryption include 2048 bits or higher for robust security. Larger key sizes provide increased resistance to attacks, especially with advances in computing power. It's important to select an appropriate key size to balance security and performance based on the specific application and security requirements. Unlike symmetric ciphers, RSA does not use a fixed block size since the block size is determined by the input data's size.

TASK 1.4

The entropy values increased after encryption for all algorithms. Among these, the DES and IDEA algorithms demonstrated the least increase in entropy when dealing with homogenous text. Encrypted text generated by these algorithms tends to reveal characteristics of the original text, such as repeated letters, which is evident in the histograms.

On the other hand, the AES algorithm significantly increased the entropy, approaching the maximum possible value. In this case, it becomes nearly impossible to discern the nature of the original text with the naked eye, as the histograms display a more uniform distribution of characters, making it challenging to identify any patterns.

For text that is moderately diverse in content, the AES algorithm also exhibited a substantial increase in entropy, although the difference from the other algorithms was less pronounced compared to homogenous text. Encrypted texts using IDEA and DES algorithms still showed variations in character frequency, as indicated by the histograms, but these differences were more subtle than in the case of homogenous text.

In the scenario of regular text, the entropy increased in all three analysed algorithms, reaching similar levels, close to the maximum achievable entropy. The histograms displayed a comparable distribution of characters, highlighting a more balanced occurrence of individual characters.

TASK 1.5

In the domain of classical encryption algorithms, we observe that the entropy of the ciphertext can exhibit various behaviours. In some cases, the entropy remains constant, as seen in the Caesar cipher, while in others, it decreases, as exemplified by the ADFGVX cipher. The extent to which entropy increases is closely tied to the length and complexity of the encryption key. Notably, the shape of histograms often remains consistent, with only shifts along the horizontal axis, providing clues about the specific encryption method employed.

For block ciphers, there is a consistent trend of significantly increasing entropy. This substantial boost in entropy poses a formidable challenge for cryptanalysts, rendering traditional methods like histogram analysis less effective and sometimes even inadequate for breaking the ciphertext. The behaviour of the ciphertext entropy varies across these encryption algorithms, and these distinctive patterns can reveal which algorithm was employed in the encryption process.

TASK 1.6

For IDEA and DES, both of which have a fixed block size of 64 bits (8 bytes), we observed that the entropy of the ciphertext increased less when dealing with homogenous text. This is because with a smaller block size, the encryption process might have difficulty masking the patterns in the original text, resulting in lower entropy.

On the other hand, AES uses a larger fixed block size of 128 bits (16 bytes). As a result, when AES was employed, we noted a significant increase in the entropy of the ciphertext. The larger block size allowed for more extensive mixing and substitution of data during encryption, making it challenging to discern patterns in the original text and resulting in higher entropy.

TASK 1.7

In the case of the AES algorithm, where it is possible to alter the key length, a slight increase in key length leads to a marginal improvement in the entropy of the encrypted data. However, this difference is so negligible that it remains imperceptible both in the textual representation and when examining histograms.

TASK 1.8

The entropy of the encrypted data is significantly influenced by the entropy of the plaintext. This influence is particularly prominent when considering the IDEA and DES algorithms. Nevertheless, empirical observations indicate that, with respect to the AES algorithm, this relationship does not carry substantial weight, as the entropy remains consistently high for both uniform and varied texts.

TASK 1.9

The choice of encryption algorithm has a significant impact on the resulting ciphertext's entropy, as evident from the information provided.

When using the DES algorithm, the ciphertext exhibited relatively lower entropy, particularly when applied to homogenous text. This suggests that DES may not be as effective at masking patterns in the original text, making it easier to discern, and resulting in lower entropy.

IDEA, another encryption algorithm, showed a slightly better performance in terms of increasing entropy compared to DES, but it still had limitations, especially when dealing with homogenous text.

In contrast, the AES algorithm consistently demonstrated a significant increase in ciphertext entropy. It approached the maximum possible entropy, making it challenging to identify patterns in the original text, regardless of the type of text content.

TASK 2.1

Text 1

It is homogeneous text which consist of 1500 characters of letter “v”

Text 2

Sequence of characters “csgo” repeated

Text 3

Wake up to reality! Nothing ever goes as planned in this accursed world. The longer you live, the more you realize that the only things that truly exist in this reality are merely pain. suffering and futility. Listen, everywhere you look in this world, wherever there is light, there will always be shadows to be found as well. As long as there is a concept of victors, the vanquished will also exist. The selfish intent of wanting to preserve peace initiates war. and hatred is born in order to protect love. There are nexuses causal relationships that cannot be separated

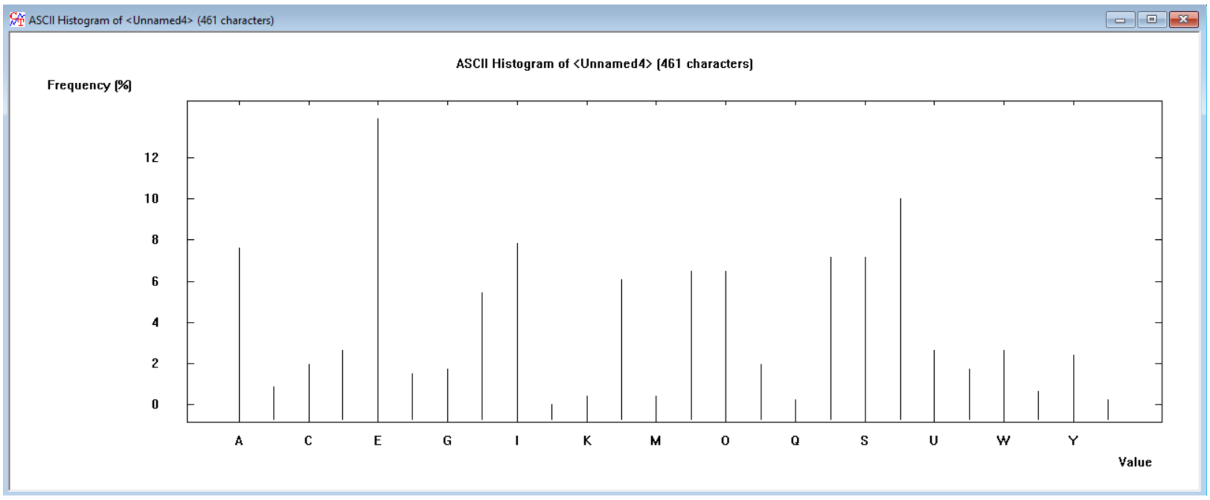
TASK 2.2

For encrypting process the AES algorithm will be used. 128 bit key will be used for encrypting

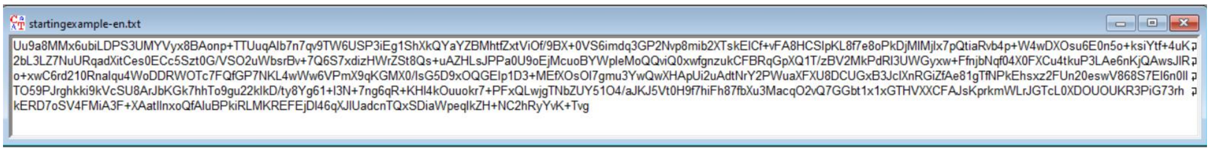
Key: 2164239413FCDB4209F24028CCFAE0FB

Plaintext:

Entropy: 4.09

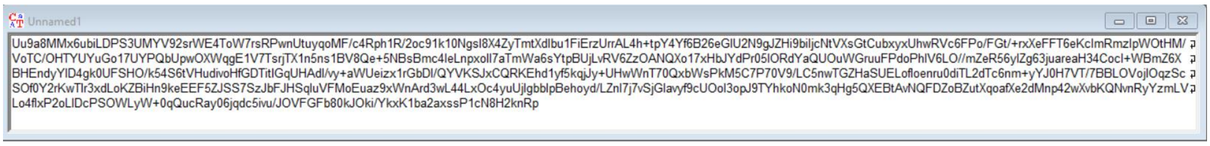


CBC:



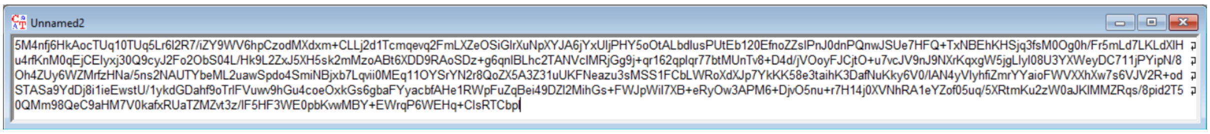
Uu9a8MMx6ubiLDPS3UMYVyx8BAonp+TTUuqAlb7n7qv9TW6USP3iEg1ShXkQYaYZBMhtfZxtViOf/9BX+0VS6imdq3GP2Nvp8mib2XTskElCf+vFA8HCSlpKL8f7e8oPkDjMlMjlx7pQtiaRvb4p+W4wDXOsu6E0n5o+ksiYtf+4uK
2bL3LZ7NuURqadXitCes0ECc5Szt0G/VSO2uWbsrBv+7Q6S7xdizHWrZSt8Qs+uAZHLsJPPa0U9oEjMcuoBYWpleMoQQviQ0xwfgnzukCFBRqGpXQ1T/zBV2MkPdRl3UWGyxw+FfnjbNqf04X0FXCu4tkuP3LAe6nKjQAwsJlR
o+xwC6rd210Rnalqu4WoDDRWOTc7FQfGP7NKL4wWw6VPmX9qKGMX0/IsG5D9xOQGElp1D3+MEfXOsOl7gmu3YwQwXHApUi2uAdtNrY2PWuaXFXU8DCUGxB3JclXnRGiZfAe81gTfNPkEhsxz2FUn20eswV868S7El6n0ll
TO59PJrghkki9kVcSU8ArJbKGk7hhTo9gu22klkD/ty8Yg61+I3N+7ng6qR+KHl4kOuuokr7+PFxQLwjgTNbZUY51O4/aJKJ5Vt0H9f7hiFh87fbXu3MacqO2vQ7GGbt1x1xGTHVXXCFAJsKprkmWLrJGTcL0XDOUOUKR3PiG73rh
kERD7oSV4FMiA3F+XAatlInxoQfAluBPkiRLMKREFEjDl46qXJlUadcnTQxSDiaWpeqlkZH+NC2hRyYvK+Tvg

ECB:



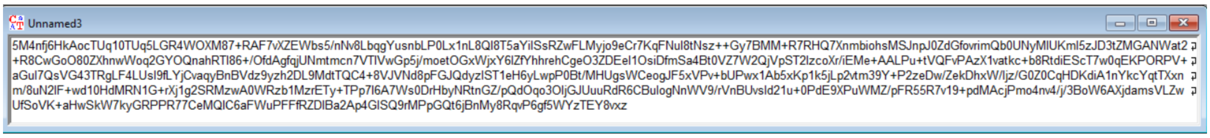
Uu9a8MMx6ubiLDPS3UMYV92srWE4ToW7rsRPwnUtuyqoMF/c4Rph1R/2oc91k10Ngsl8X4ZyTmtXdlbu1FiErzUrrAL4h+tpY4Yf6B26eGlU2N9gJZHi9biljcNtVXsGtCubxyxUhwRVc6FPo/FGt/+rxXeFFT6eKclmRmzlpWOtHM/
VoTC/OHTYUYuGo17UYPQbUpwOXWqgE1V7TsrjTX1n5ns1BV8Qe+5NBsBmc4leLnpxoll7aTmWa6sYtpBUjLvRV6ZzOANQXo17xHbJYdPr05lORdYaQUOuWGruuFPdoPhlV6LO//mZeR56ylZg63juareaH34Cocl+WBmZ6X
BHEndyYlD4gk0UFSHO/k54S6tVHudivoHfGDTitlGqUHAdl/vy+aWUeizx1rGbDl/QYVKSJxCQRKEhd1yf5kqjJy+UHwWnT70QxbWsPkM5C7P70V9/LC5nwTGZHaSUELofloenru0diTL2dTc6nm+yYJ0H7VT/7BBLOVojlOqzSc
SOf0Y2rKwTlr3xdLoKZBiHn9keEEF5ZJSS7SzJbFJHSqluVFMoEuaz9xWnArd3wL44LxOc4yuUjlgbblpBehoyd/LZnl7j7vSjGlavyf9cUOol3opJ9TYhkoN0mk3qHg5QXEBtAvNQFDZoBZutXqoafXe2dMnp42wXvbKQNvnRyYzmLV
Lo4flxP2oLIDcPSOWLyW+0qQucRay06jqdc5ivu/JOVFGFb80kJOki/YkxK1ba2axssP1cN8H2knRp

OFB:



5M4nfj6HkAocTUq10TUq5Lr6l2R7/iZY9WV6hpCzodMXdxm+CLLj2d1Tcmqevq2FmLXZeOSiGlrXuNpXYJA6jYxUljPHY5oOtALbdlusPUtEb120EfnoZZslPnJ0dnPQnwJSUe7HFQ+TxNBEhKHSjq3fsM0Og0h/Fr5mLd7LKLdXlH
u4rfKnM0qEjCElyxj30Q9cyJ2Fo2ObS04L/Hk9L2ZxJ5XH5sk2mMzoABt6XDD9RAoSDz+g6qnlBLhc2TANVclMRjGg9j+qr162qplqr77btMUnTv8+D4d/jVOoyFJCjtO+u7vcJV9nJ9NXrKqxgW5jgLlyl08U3YXWeyDC711jPYipN/8
Oh4ZUy6WZMrfzHNa/5ns2NAUTYbeML2uawSpdo4SmiNBjxb7Lqvii0MEq11OYSrYN2r8QoZX5A3Z31uUKFNeazu3sMSS1FCbLWRoXdXJp7YkKK58e3taihK3DafNuKky6V0/lAN4yVlyhfiZmrYYaioFWVXXhXw7s6VJV2R+od
STASa9YdDj8i1ieEwstU/1ykdGDahf9oTrlFVuwv9hGu4coeOxkGs6gbaFYyacbfAHe1RWpFuZqBei49DZl2MihGs+FWJpWil7XB+eRyOw3APM6+DjvO5nu+r7H14j0XVNhRA1eYZof05uq/5XRtmKu2zW0aJKlMMZRqs/8pid2T5
0QMm98QeC9aHM7V0kafxRUaTZMZvt3z/lF5HF3WE0pbKwwMBY+EWrqP6WEHq+ClsRTCbp

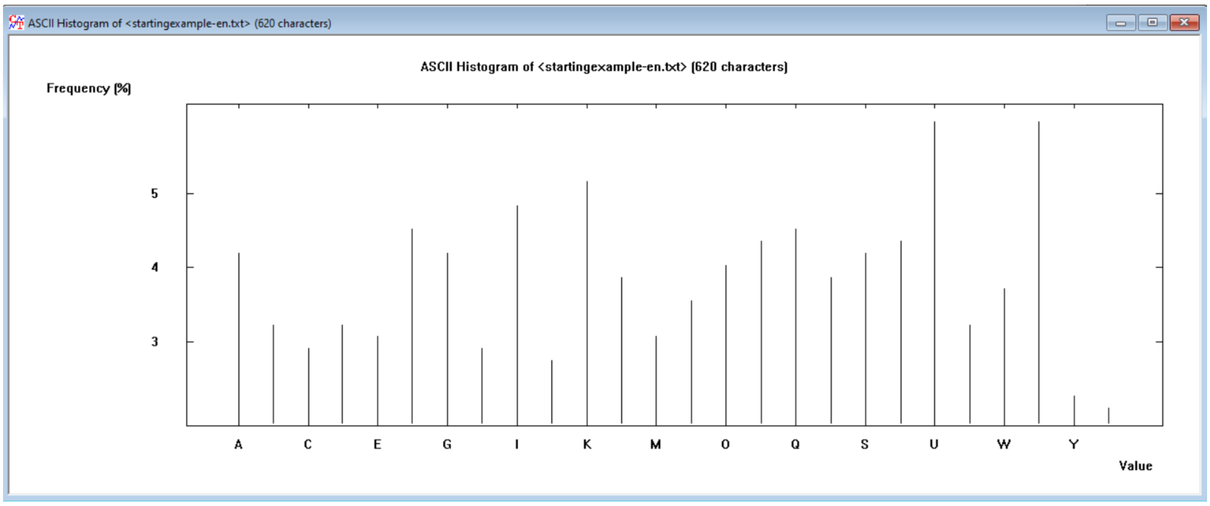
CFB:



5M4nfj6HkAocTUq10TUq5LGR4WOXM87+RAF7vXZEWbs5/nNv8LbqgYusnbLP0Lx1nL8Ql8T5aYilSsRZwFLMyjo9eCr7KqFNul8tNsz++Gy7BMM+R7RHQ7XnmbiohsMSJnpJ0ZdGfovrimQb0UNyMlUKml5zJD3tZMGANWat2
+R8CwGoO80ZXhnwWoq2GYOQnahRTl86+/OfdAgfqjUNmtmcn7VTlVwGp5j/moetOGxWjxY6lZfYhhrehCgeO3ZDEel1OsiDfmSa4Bt0VZ7W2QjVpST2lzcoXr/iEMe+AALPu+tVQFvPAzX1vatkc+b8RtdiEScT7w0qEKPORPV+
aGul7QsVG43TRgLF4LUsl9fLYjCvaqyBnBVdz9yzh2DL9MdtTQC4+8VJVNd8pFGJQdyzlST1eH6yLwpP0Bt/MHUgsWCeogJF5xVPv+bUPwx1Ab5xKp1k5jLp2vtm39Y+P2zeDw/ZekDhxW/ljz/G0Z0CqHDKdiA1nYkcYqtTXxn
m/8uN2lF+wd10HdMRN1G+rXj1g2SRMzwA0WRzb1MzrETy+TPp7l6A7Ws0DrHbyNRtnGZ/pQdOqo3OljGJUuuRdR6CBulogNnWV9/rVnBUvsld21u+0PdE9XPuWMZ/pFR55R7v19+pdMAcjPmo4nv4/j/3BoW6AXjdamsVLZw
UfSoVK+aHwSkW7kyGRPPR77CeMQlC6aFWuPFFfRZDlBa2Ap4GlSQ9rMPpGQt6jBnMy8RqvP6gf5WYzTEY8vxz

Entropy comparison		
Algorithm	Ciphertext	Plaintext
CBC	4.65	4.09
ECB	4.66	
OFB	4.67	
CFB	4.67	

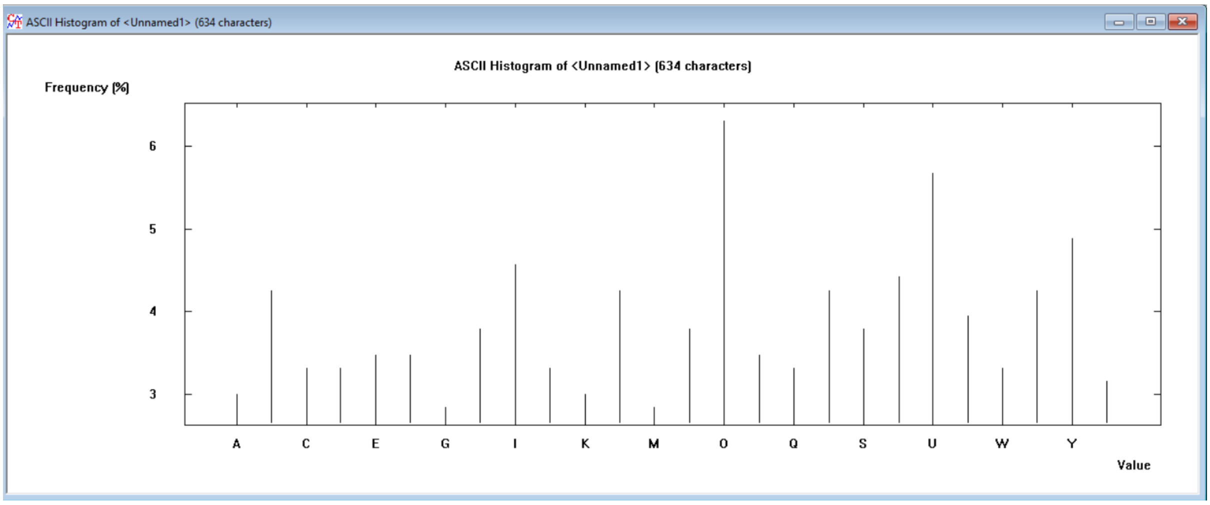
CBC:



ASCII Histogram of <startingexample-en.txt> (620 characters)

ASCII Histogram of <startingexample-en.txt> (620 characters)

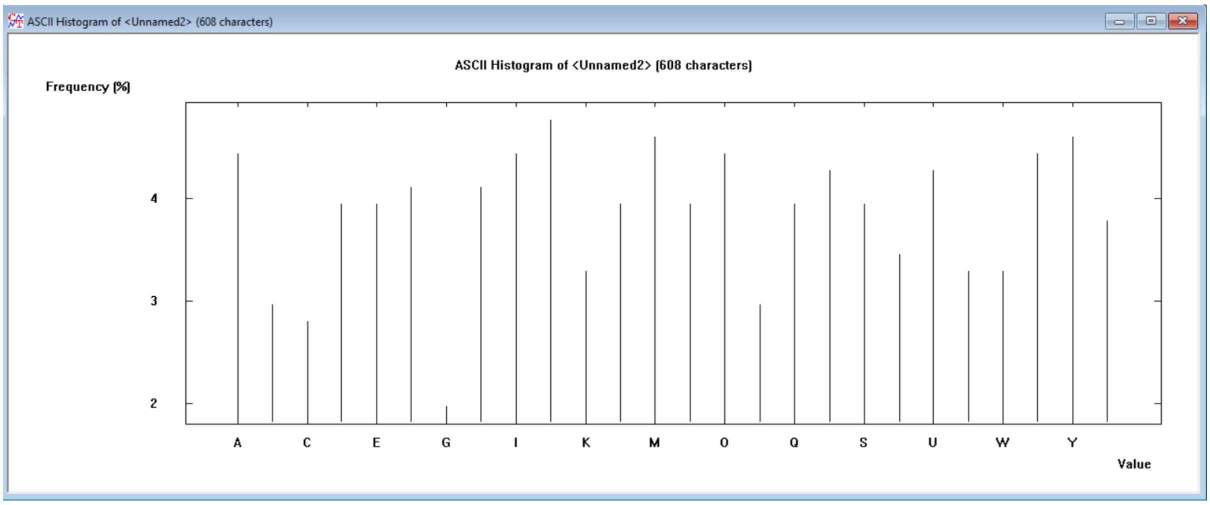
ECB:



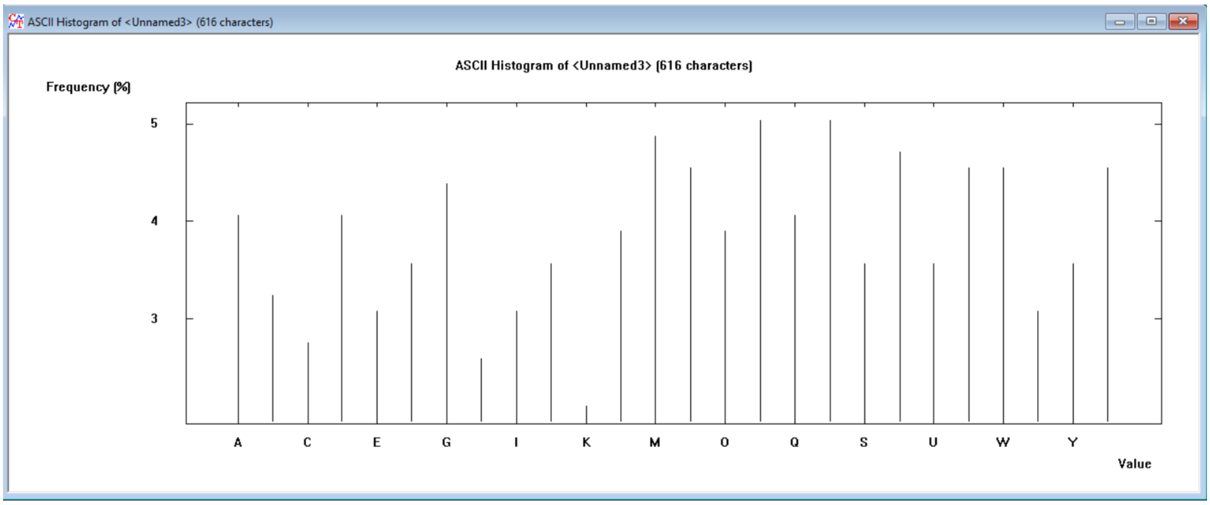
ASCII Histogram of <Unnamed1> (634 characters)

ASCII Histogram of <Unnamed1> (634 characters)

OFB:


ASCII Histogram of <Unnamed2> (608 characters)
ASCII Histogram of <Unnamed2> (608 characters)
Frequency (%)
4
3
2
A
C
E
G
I
K
M
O
Q
S
U
W
Y
Value

CFB:

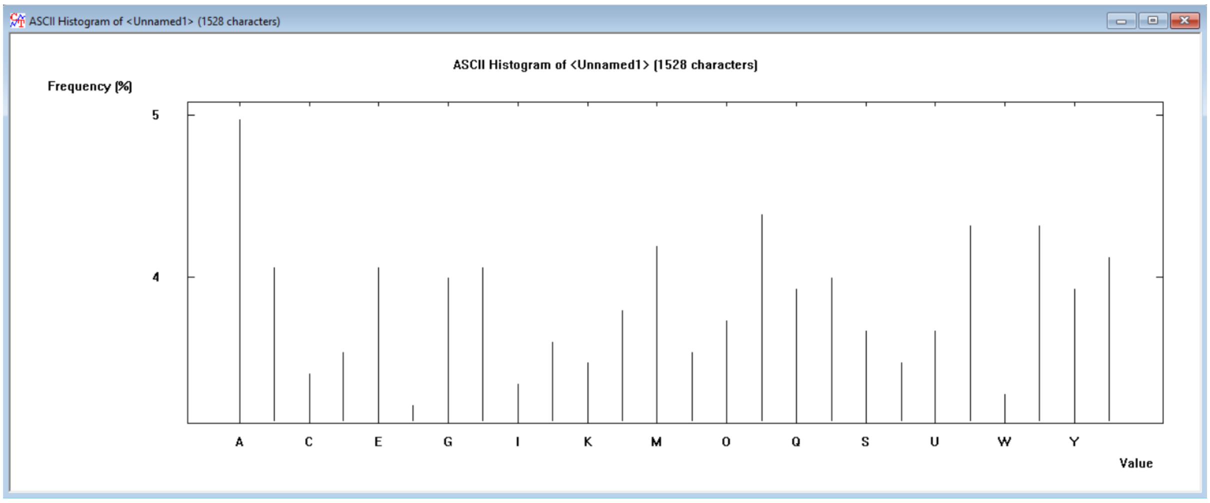

ASCII Histogram of <Unnamed3> (616 characters)
ASCII Histogram of <Unnamed3> (616 characters)
Frequency (%)
5
4
3
A
C
E
G
I
K
M
O
Q
S
U
W
Y
Value

TASK 2.4

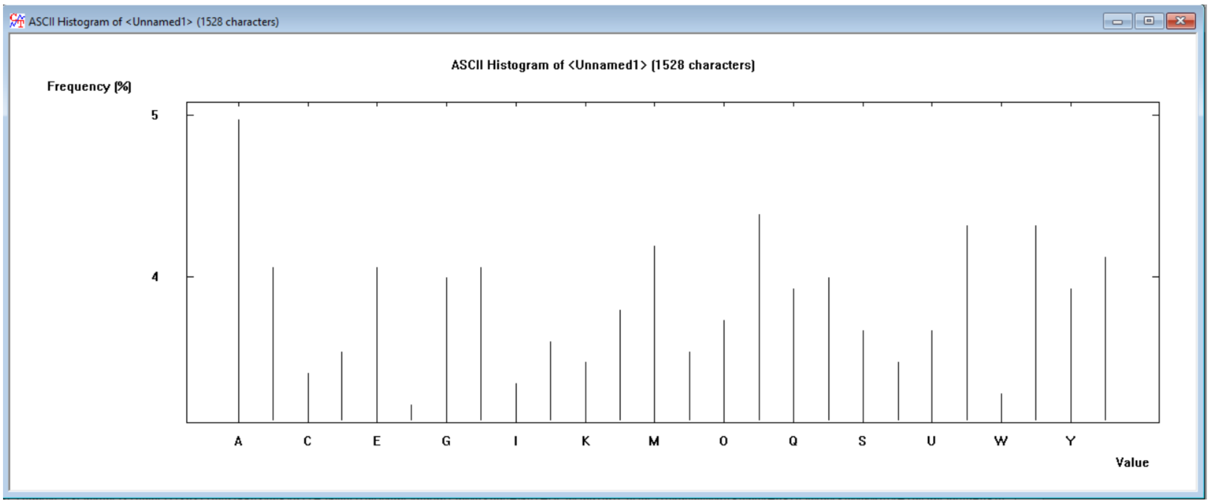
abcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcd
abcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcd
abcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcd
abcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcd
abcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcd
abcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcd
abcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcd
abcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcd
abcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcd
abcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcd
abcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcd
abcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcd
abcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcd
abcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcd
abcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcd
abcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcd
abcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcd

Entropy comparison		
Algorithm	Ciphertext	Plaintext
CBC	4.69	2
ECB	4.34	
OFB	4.68	
CFB	4.68	

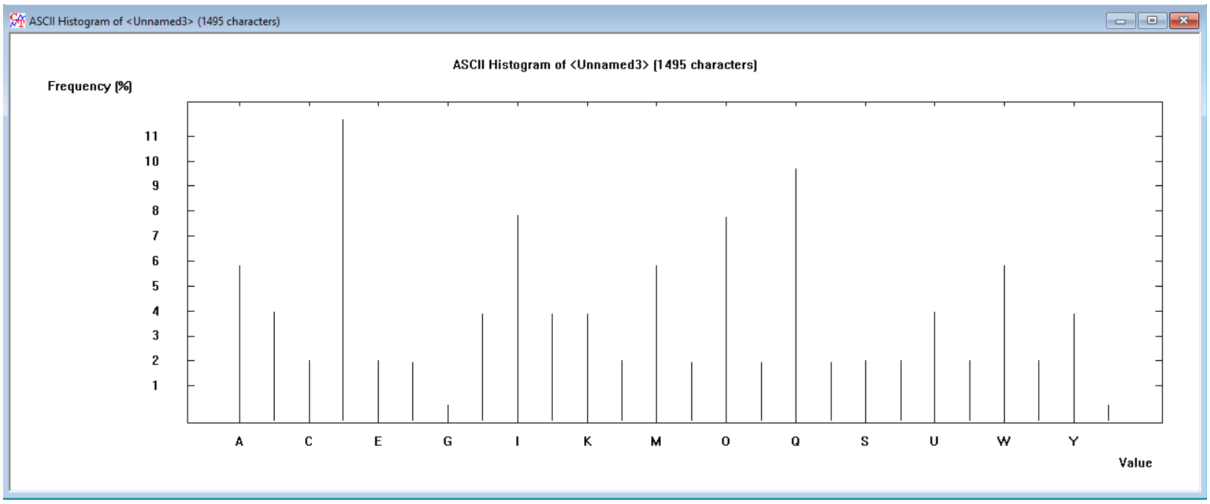
AES(CBC):



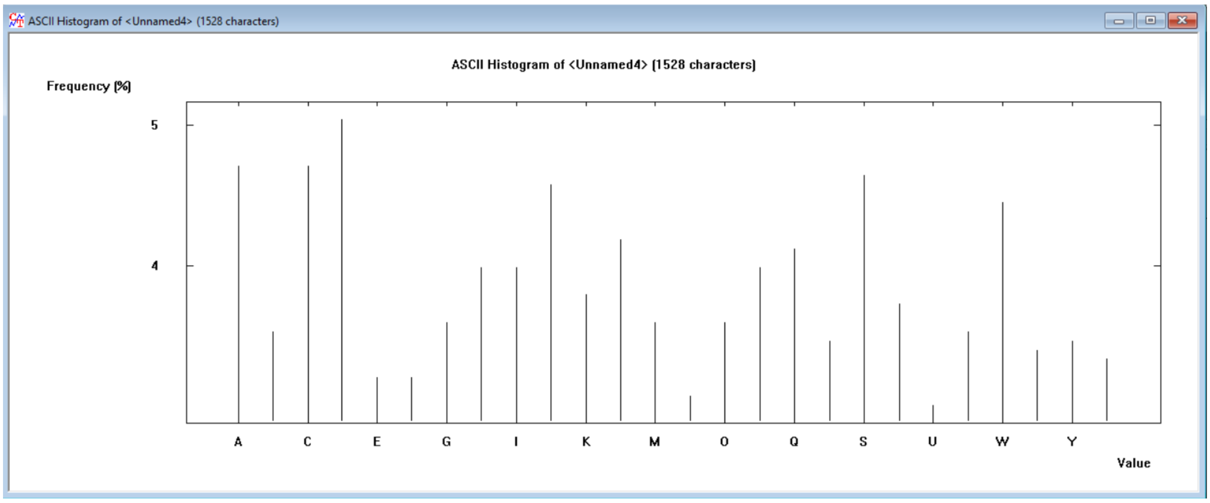
AES(CFB):



AES(ECB):



AES(OFB):



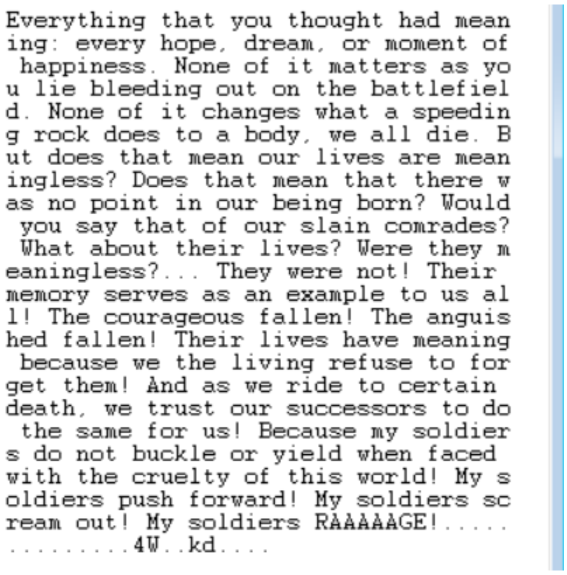
The ECB mode exhibited the poorest encryption performance when applied to uniform text, as it resulted in evident patterns of repeated text blocks in the ciphertext. In contrast, the CBC, OFB, and CFB modes demonstrated significantly superior performance, as they effectively concealed the plaintext contents. Each of these three modes delivered similarly commendable results in terms of high entropy and well-aligned histograms.

TASK 2.5

Text: Everything that you thought had meaning: every hope, dream, or moment of happiness. None of it matters as you lie bleeding out on the battlefield. None of it changes what a speeding rock does to a body, we all die. But does that mean our lives are meaningless? Does that mean that there was no point in our being born? Would you say that of our slain comrades? What about their lives? Were they meaningless?... They were not! Their memory serves as an example to us all! The courageous fallen! The anguished fallen! Their lives have meaning because we the living refuse to forget them! And as we ride to certain death, we trust our successors to do the same for us! Because my soldiers do not buckle or yield when faced with the cruelty of this world! My soldiers push forward! My soldiers scream out! My soldiers RAAAAAGE!

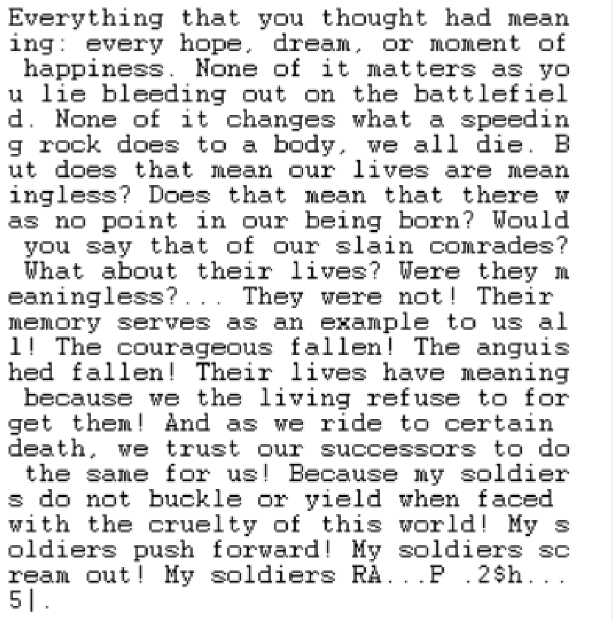
AES(CBC):

Adding one byte:



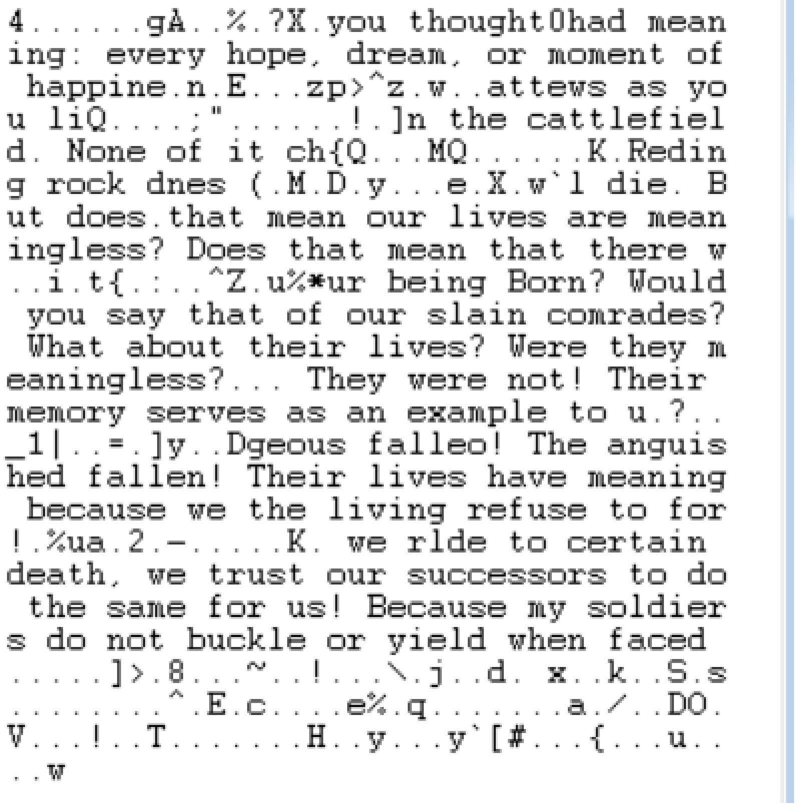
```
Everything that you thought had mean
ing: every hope, dream, or moment of
 happiness. None of it matters as yo
u lie bleeding out on the battlefiel
d. None of it changes what a speedin
g rock does to a body, we all die. B
ut does that mean our lives are mean
ingless? Does that mean that there w
as no point in our being born? Would
 you say that of our slain comrades?
 What about their lives? Were they m
eaningless?... They were not! Their 
memory serves as an example to us al
l! The courageous fallen! The anguis
hed fallen! Their lives have meaning
 because we the living refuse to for
get them! And as we ride to certain 
death, we trust our successors to do
 the same for us! Because my soldier
s do not buckle or yield when faced 
with the cruelty of this world! My s
oldiers push forward! My soldiers sc
ream out! My soldiers RAAAAAGE!.....
..........4W..kd....
```

Removing one byte:



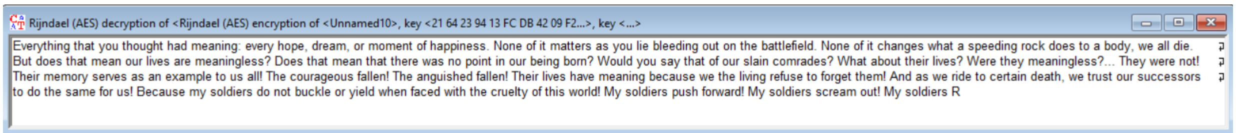
```
Everything that you thought had mean
ing: every hope, dream, or moment of
 happiness. None of it matters as yo
u lie bleeding out on the battlefiel
d. None of it changes what a speedin
g rock does to a body, we all die. B
ut does that mean our lives are mean
ingless? Does that mean that there w
as no point in our being born? Would
 you say that of our slain comrades?
 What about their lives? Were they m
eaningless?... They were not! Their 
memory serves as an example to us al
l! The courageous fallen! The anguis
hed fallen! Their lives have meaning
 because we the living refuse to for
get them! And as we ride to certain 
death, we trust our successors to do
 the same for us! Because my soldier
s do not buckle or yield when faced 
with the cruelty of this world! My s
oldiers push forward! My soldiers sc
ream out! My soldiers RA...P .2$h...
5|.
```

change one each or several bits in different bytes (close or far apart):



```
4......gA..%.?X.you thought0had mean
ing: every hope, dream, or moment of
 happine.n.E...zp>^z.w..attews as yo
u liQ....;"......!.]n the cattlefiel
d. None of it ch{Q...MQ......K.Redin
g rock dnes (.M.D.y...e.X.w`l die. B
ut does.that mean our lives are mean
ingless? Does that mean that there w
..i.t{.:..^Z.u%*ur being Born? Would
 you say that of our slain comrades?
 What about their lives? Were they m
eaningless?... They were not! Their 
memory serves as an example to u.?..
_1|..=.]y..Dgeous falleo! The anguis
hed fallen! Their lives have meaning
 because we the living refuse to for
!.%ua.2.-.....K. we rlde to certain 
death, we trust our successors to do
 the same for us! Because my soldier
s do not buckle or yield when faced 
.....]>.8...~..!...\.j..d. x..k..S.s
........^.E.c....e%.q.......a./..DO.
V...!..T.......H..y...y`[#...{...u..
..w
```

Removing a piece of ciphertext equal to the length of the algorithm block(128 bits – 16bytes)



Rijndael (AES) decryption of <Rijndael (AES) encryption of <Unnamed10>, key <21 64 23 94 13 FC DB 42 09 F2...>, key <...>

```
Everything that you thought had meaning: every hope, dream, or moment of happiness. None of it matters as you lie bleeding out on the battlefield. None of it changes what a speeding rock does to a body, we all die.
But does that mean our lives are meaningless? Does that mean that there was no point in our being born? Would you say that of our slain comrades? What about their lives? Were they meaningless?... They were not!
Their memory serves as an example to us all! The courageous fallen! The anguished fallen! Their lives have meaning because we the living refuse to forget them! And as we ride to certain death, we trust our successors
to do the same for us! Because my soldiers do not buckle or yield when faced with the cruelty of this world! My soldiers push forward! My soldiers scream out! My soldiers R
```

TASK 2.6

A) The encrypted text's visual characteristics strongly indicate the utilization of ECB mode. This inference is drawn from the conspicuous cyclic repetition of a 32-character group within the text. Prior experiments have substantiated that when employing the ECB mode for encrypting uniform text, these cyclic repetitions emerge consistently. Consequently, it can be deduced that the block size is 64 bytes.

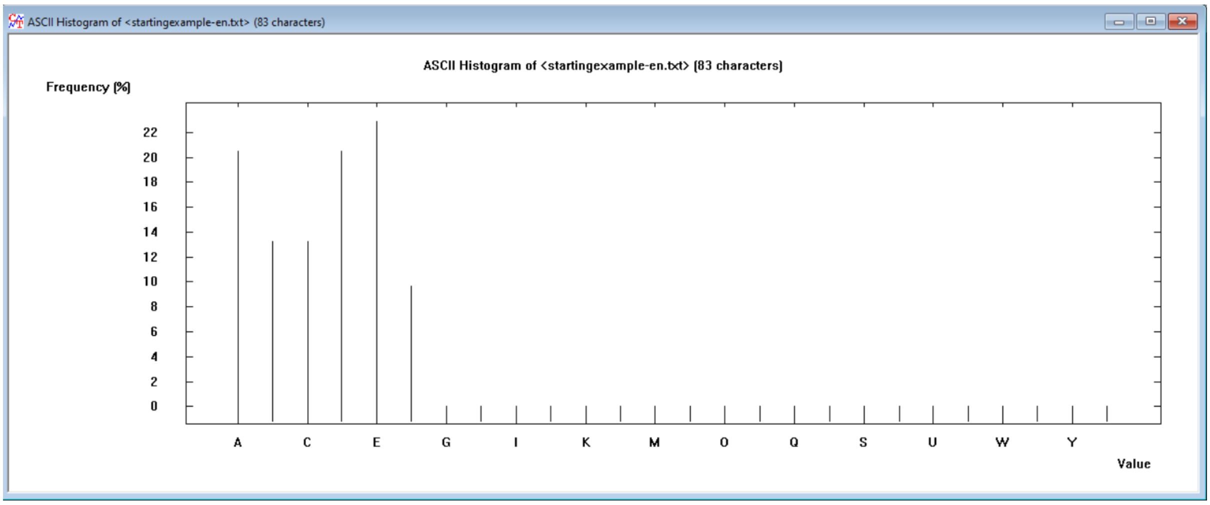
b)

This text also shows cyclic repetition of letter strings, this time every 64 characters.

This suggests the use of ECB mode again for encryption, except that now the algorithm block

has been lengthened twice, to 128 bytes.

c)

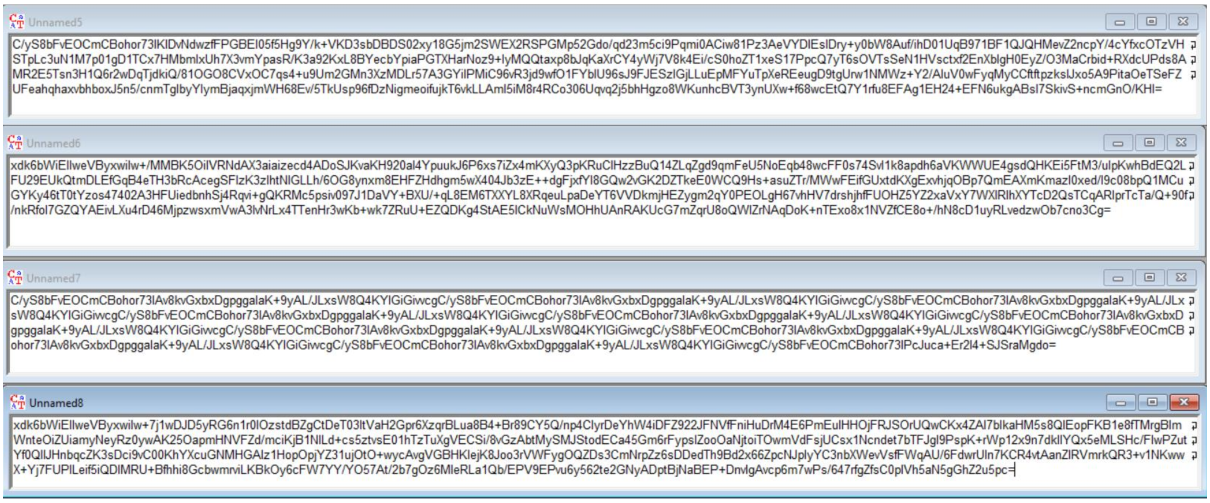


At first glance, the text doesn't exhibit an apparent cyclic repetition of letter sequences. However, the relatively low entropy(2.52/4.70) and misaligned histogram hint at the possible use of a less robust encryption algorithm, such as IDEA, combined with ECB or CBC mode. Nevertheless, due to the absence of discernible cyclic patterns, determining the algorithm's block length remains a challenging task. It's worth noting that the text's appearance might also be influenced by its inherent characteristics, potentially featuring minimal variation.

TASK 2.7

Vvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvv vvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvv vvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvv vvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvv vvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvv vvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvv

Entropy comparison		
Algorithm	Ciphertext	Plaintext
CBC	4.67	0
ECB	4.19	
OFB	4.68	
CFB	4.67	



```
C/yS8bFvEOCmCBohor73lKIDvNdwzfFPGBEI05f5Hg9Y/k+VKD3sbDBDS02xy18G5jm2SWEX2RSPGMp52Gdo/qd23m5ci9Pqmi0ACiw81Pz3AeVYDlEslDry+y0bW8Auf/ihD01UqB971BF1QJQHMevZ2ncpY/4cYfxcOTzVH
STpLc3uN1M7p01gD1TCx7HMbmlxUh7X3vmYpasR/K3a92KxL8BYecbYpiaPGTXHarNoz9+lyMQQtaxp8bJqKaXrCY4yWj7V8k4Ei/cS0hoZT1xeS17PpcQ7yT6sOVTsSeN1HVsctxf2EnXblgH0EyZ/O3MaCrbid+RXdcUPds8A
MR2E5Tsn3H1Q6r2wDqTjdkiQ/81OGO8CVxOC7qs4+u9Um2GMn3XzMDLr57A3GYilPMiC96vR3jd9wfO1FYblU96sJ9FJESzlGjLLuEpMFYuTpXeREeugD9tgUrw1NMWz+Y2/AluV0wFyqMyCCftftpzkslJxo5A9PitaOeTSeFZ
UFeahqhaxvbhboxJ5n5/cnmTglbyYlymBjaqxjmWH68Ev/5TkUsp96fDzNigmeoifujkT6vkLLAml5iM8r4RCo306Uqvq2j5bhHgzo8WKunhcBVT3ynUXw+f68wcEtQ7Y1rfu8EFAg1EH24+EFN6ukgABsl7SkivS+ncmGnO/KHI=
```

```
xdk6bWiEllweVByxwilw+/MMBK5OilVRNdAX3aiaizecd4ADoSJKvaKH920al4YpuukJ6P6xs7iZx4mKXyQ3pKRuClHzzBuQ14ZLqZgd9qmFeU5NoEqb48wcFF0s74Svl1k8apdh6aVKWWUE4gsdQHKEi5FtM3/ulpKwhBdEQ2L
FU29EUkQtmDLEfGqB4eTH3bRcAcegSFlzK3zlhtNIGLLh/6OG8ynxm8EHFZHdhgm5wX404Jb3zE++dgFjxfYl8GQw2vGK2DZTkeE0WCQ9Hs+asuZTr/MWwFEifGUxtdKXgExvhjqOBp7QmEAXmKmazl0xed/l9c08bpQ1MCu
GYKy46tT0tYzos47402A3HFUiedbnhSj4Rqvi+gQKRMc5psiv097J1DaVY+BXU/+qL8EM6TXXYL8XRqeuLpaDeYT6VVDkmjHEZygm2qY0PEOLgH67vhHV7drshjhfFUOHZ5YZ2xaVxY7WXlRlhXYTcD2QsTCqARlprTcTa/Q+90f
/nkRfol7GZQYAEivLXu4rD46MjpzwsxmVwA3lvNrLx4TTenHr3wKb+wk7ZRuU+EZQDKg4StAE5lCkNuWsMOHhUAnRAKUcG7mZqrU8oQWlZrNAqDoK+nTExo8x1NVZfCE8o+/hN8cD1uyRLvedzwOb7cno3Cg=
```

```
C/yS8bFvEOCmCBohor73lAv8kvGxbxDgpggalaK+9yAL/JLxsW8Q4KYlGiGiwcgC/yS8bFvEOCmCBohor73lAv8kvGxbxDgpggalaK+9yAL/JLxsW8Q4KYlGiGiwcgC/yS8bFvEOCmCBohor73lAv8kvGxbxDgpggalaK+9yAL/JLx
sW8Q4KYlGiGiwcgC/yS8bFvEOCmCBohor73lAv8kvGxbxDgpggalaK+9yAL/JLxsW8Q4KYlGiGiwcgC/yS8bFvEOCmCBohor73lAv8kvGxbxDgpggalaK+9yAL/JLxsW8Q4KYlGiGiwcgC/yS8bFvEOCmCBohor73lAv8kvGxbxD
gpggalaK+9yAL/JLxsW8Q4KYlGiGiwcgC/yS8bFvEOCmCBohor73lAv8kvGxbxDgpggalaK+9yAL/JLxsW8Q4KYlGiGiwcgC/yS8bFvEOCmCBohor73lAv8kvGxbxDgpggalaK+9yAL/JLxsW8Q4KYlGiGiwcgC/yS8bFvEOCmCB
ohor73lAv8kvGxbxDgpggalaK+9yAL/JLxsW8Q4KYlGiGiwcgC/yS8bFvEOCmCBohor73lAv8kvGxbxDgpggalaK+9yAL/JLxsW8Q4KYlGiGiwcgC/yS8bFvEOCmCBohor73lPcJuca+Er2l4+SJSraMgdo=
```

```
xdk6bWiEllweVByxwilw+7j1wDJD5yRG6n1r0lOzstdBZgCtDeT03ltVaH2Gpr6XzqrBLua8B4+Br89CY5Q/np4ClyrDeYhW4iDFZ922JFNVfFniHuDrM4E6PmEulHHOjFRJSOrUQwCKx4ZAl7blkaHM5s8QlEopFKB1e8fTMrgBlm
WnteOiZUiamyNeyRz0ywAK25OapmHNVFZd/mciKjB1NlLd+cs5ztvsE01hTzTuXgVECSi/8vGzAbtMySMJStodECa45Gm6rFypslZooOaNjtoiTOwmVdFsjUCsx1Ncndet7bTFJgl9PspK+rWp12x9n7dklIYQx5eMLSHc/FlwPZut
Yf0QlJHnbqcZK3sDci9vC00KhYXcuGNMHGAlz1HopOpjYZ31ujOtO+wycAvgVGBHKlejK8Joo3rVWFygOQZDs3CmNrpZz6sDDedTh9Bd2x66ZpcNJplyYC3nbXWevVsfFWqAU/6FdwrUln7KCR4vtAanZlRVmrkQR3+v1NKww
X+Yj7FUPlLeif5iQDlMRU+Bfhhi8GcbwmrviLKBkOy6cFW7YY/YO57At/2b7gOz6MleRLa1Qb/EPV9EPvu6y562te2GNyADptBjNaBEP+DnvlgAvcp6m7wPs/647rfgZfsC0plVh5aN5gGhZ2u5pc=
```

In the case of ECB mode, there is a notable lack of entropy, resulting in distinct cyclic repetitions of letter strings within the cryptogram. In contrast, for ECB, OFB, and CFB modes, the entropy level is significantly increased, approaching the maximum achievable entropy. Consequently, cryptograms generated using these modes do not divulge any discernible patterns or characteristics of the plaintext content.

TASK 2.8

Adding one byte at the end:

Adding a single byte at the end of the ciphertext will have a localized impact. It will corrupt the last decrypted plaintext block corresponding to that byte. The rest of the plaintext will remain intact.

Removing one byte:

Removing a byte from the ciphertext will affect the last decrypted plaintext block. The decrypted plaintext will have one byte missing at the end.

Changing one or several bits in different bytes (close or far apart):

Changing one or several bits in different bytes of the ciphertext will result in corresponding changes in the decrypted plaintext. The impact is localized to the bits that were changed in the ciphertext.

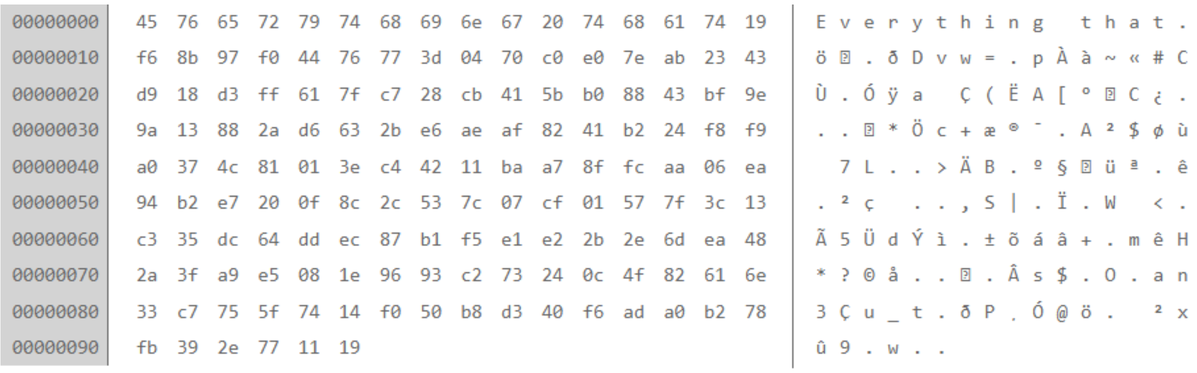
Removing a piece of ciphertext equal to the length of the algorithm block (128 bits or 16 bytes):

Removing a block-sized chunk of ciphertext (16 bytes) will result in the loss of an entire plaintext block. This means the corresponding plaintext block will be completely unrecoverable, and subsequent blocks will be affected by the error propagation.

TASK 2.9

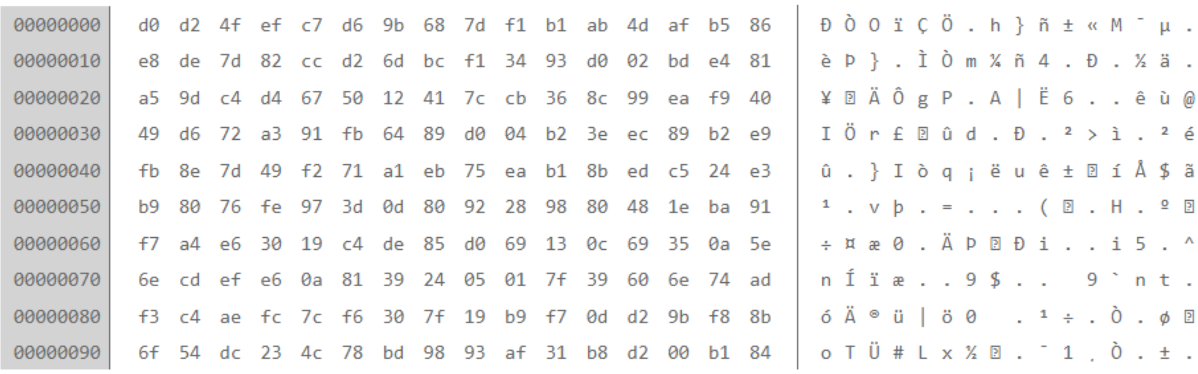
Removing one byte in each block:

AES(CFB):



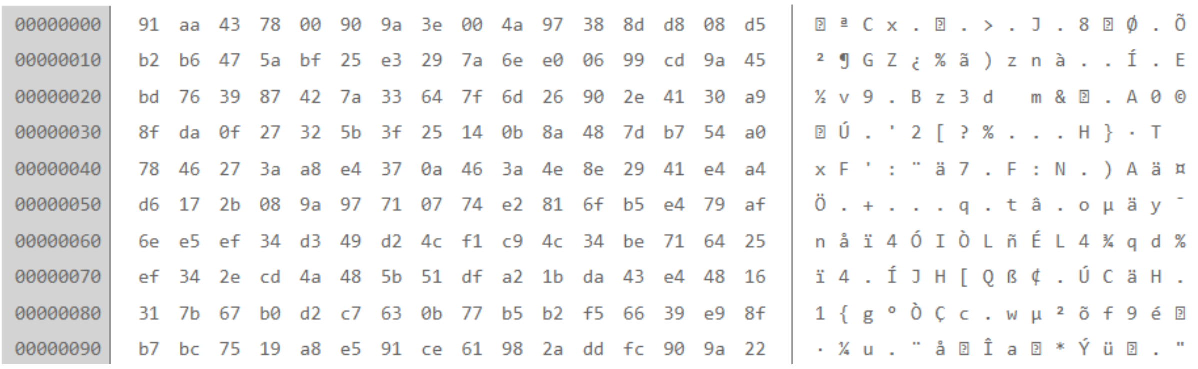
```
00000000  45 76 65 72 79 74 68 69 6e 67 20 74 68 61 74 19  | Everything that.
00000010  f6 8b 97 f0 44 76 77 3d 04 70 c0 e0 7e ab 23 43  | ö⍰.ðDvw=.pÀà~«#C
00000020  d9 18 d3 ff 61 7f c7 28 cb 41 5b b0 88 43 bf 9e  | Ù.Óÿa Ç(ËA[°⍰C¿.
00000030  9a 13 88 2a d6 63 2b e6 ae af 82 41 b2 24 f8 f9  | ..⍰*Öc+æ®¯.A²$øù
00000040  a0 37 4c 81 01 3e c4 42 11 ba a7 8f fc aa 06 ea  |  7L..>ÄB.º§⍰üª.ê
00000050  94 b2 e7 20 0f 8c 2c 53 7c 07 cf 01 57 7f 3c 13  | .²ç ..,S|.Ï.W <.
00000060  c3 35 dc 64 dd ec 87 b1 f5 e1 e2 2b 2e 6d ea 48  | Ã5ÜdÝì.±õáâ+.mêH
00000070  2a 3f a9 e5 08 1e 96 93 c2 73 24 0c 4f 82 61 6e  | *?©å..⍰.Âs$.O.an
00000080  33 c7 75 5f 74 14 f0 50 b8 d3 40 f6 ad a0 b2 78  | 3Çu_t.ðP¸Ó@ö. ²x
00000090  fb 39 2e 77 11 19                                | û9.w..
```

AES(ECB):



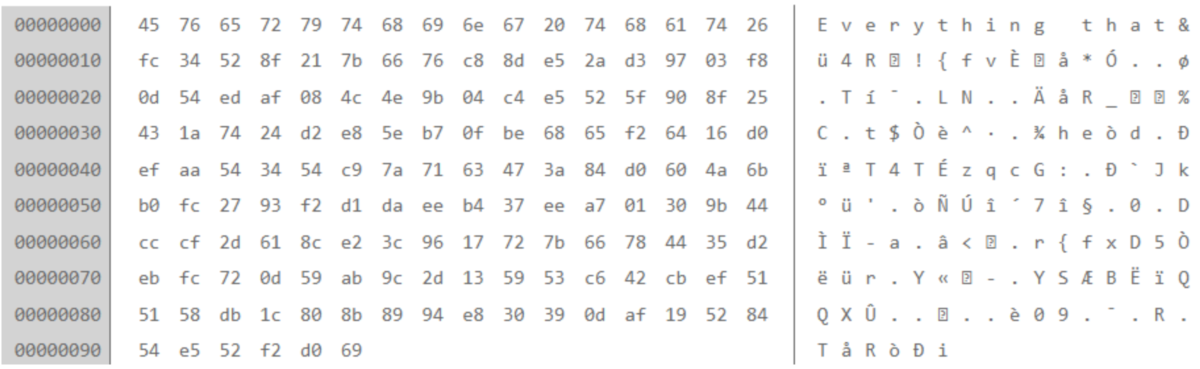
```
00000000  d0 d2 4f ef c7 d6 9b 68 7d f1 b1 ab 4d af b5 86  | ÐÒOïÇÖ.h}ñ±«M¯µ.
00000010  e8 de 7d 82 cc d2 6d bc f1 34 93 d0 02 bd e4 81  | èÞ}.ÌÒm¼ñ4.Ð.½ä.
00000020  a5 9d c4 d4 67 50 12 41 7c cb 36 8c 99 ea f9 40  | ¥⍰ÄÔgP.A|Ë6..êù@
00000030  49 d6 72 a3 91 fb 64 89 d0 04 b2 3e ec 89 b2 e9  | IÖr£⍰ûd.Ð.²>ì.²é
00000040  fb 8e 7d 49 f2 71 a1 eb 75 ea b1 8b ed c5 24 e3  | û.}Iòq¡ëuê±⍰íÅ$ã
00000050  b9 80 76 fe 97 3d 0d 80 92 28 98 80 48 1e ba 91  | ¹.vþ.=....(⍰.H.º⍰
00000060  f7 a4 e6 30 19 c4 de 85 d0 69 13 0c 69 35 0a 5e  | ÷¤æ0.ÄÞ⍰Ði..i5.^
00000070  6e cd ef e6 0a 81 39 24 05 01 7f 39 60 6e 74 ad  | nÍïæ..9$.. 9`nt.
00000080  f3 c4 ae fc 7c f6 30 7f 19 b9 f7 0d d2 9b f8 8b  | óÄ®ü|ö0 .¹÷.Ò.ø⍰
00000090  6f 54 dc 23 4c 78 bd 98 93 af 31 b8 d2 00 b1 84  | oTÜ#Lx½⍰.¯1¸Ò.±.
```

AES(CBC)



```
00000000  91 aa 43 78 00 90 9a 3e 00 4a 97 38 8d d8 08 d5  ⍰ ª C x . ⍰ . > . J . 8 ⍰ Ø . Õ
00000010  b2 b6 47 5a bf 25 e3 29 7a 6e e0 06 99 cd 9a 45  ² ¶ G Z ¿ % ã ) z n à . . Í . E
00000020  bd 76 39 87 42 7a 33 64 7f 6d 26 90 2e 41 30 a9  ½ v 9 . B z 3 d   m & ⍰ . A 0 ©
00000030  8f da 0f 27 32 5b 3f 25 14 0b 8a 48 7d b7 54 a0  ⍰ Ú . ' 2 [ ? % . . . H } · T
00000040  78 46 27 3a a8 e4 37 0a 46 3a 4e 8e 29 41 e4 a4  x F ' : ¨ ä 7 . F : N . ) A ä ¤
00000050  d6 17 2b 08 9a 97 71 07 74 e2 81 6f b5 e4 79 af  Ö . + . . . q . t â . o µ ä y ¯
00000060  6e e5 ef 34 d3 49 d2 4c f1 c9 4c 34 be 71 64 25  n å ï 4 Ó I Ò L ñ É L 4 ¾ q d %
00000070  ef 34 2e cd 4a 48 5b 51 df a2 1b da 43 e4 48 16  ï 4 . Í J H [ Q ß ¢ . Ú C ä H .
00000080  31 7b 67 b0 d2 c7 63 0b 77 b5 b2 f5 66 39 e9 8f  1 { g ° Ò Ç c . w µ ² õ f 9 é ⍰
00000090  b7 bc 75 19 a8 e5 91 ce 61 98 2a dd fc 90 9a 22  · ¼ u . ¨ å ⍰ Î a ⍰ * Ý ü ⍰ . "
```

AES(OFB):



```
00000000  45 76 65 72 79 74 68 69 6e 67 20 74 68 61 74 26  E v e r y t h i n g   t h a t &
00000010  fc 34 52 8f 21 7b 66 76 c8 8d e5 2a d3 97 03 f8  ü 4 R ⍰ ! { f v È ⍰ å * Ó . . ø
00000020  0d 54 ed af 08 4c 4e 9b 04 c4 e5 52 5f 90 8f 25  . T í ¯ . L N . . Ä å R _ ⍰ ⍰ %
00000030  43 1a 74 24 d2 e8 5e b7 0f be 68 65 f2 64 16 d0  C . t $ Ò è ^ · . ¾ h e ò d . Ð
00000040  ef aa 54 34 54 c9 7a 71 63 47 3a 84 d0 60 4a 6b  ï ª T 4 T É z q c G : . Ð ` J k
00000050  b0 fc 27 93 f2 d1 da ee b4 37 ee a7 01 30 9b 44  ° ü ' . ò Ñ Ú î ´ 7 î § . 0 . D
00000060  cc cf 2d 61 8c e2 3c 96 17 72 7b 66 78 44 35 d2  Ì Ï - a . â < ⍰ . r { f x D 5 Ò
00000070  eb fc 72 0d 59 ab 9c 2d 13 59 53 c6 42 cb ef 51  ë ü r . Y « ⍰ - . Y S Æ B Ë ï Q
00000080  51 58 db 1c 80 8b 89 94 e8 30 39 0d af 19 52 84  Q X Û . . ⍰ . . è 0 9 . ¯ . R .
00000090  54 e5 52 f2 d0 69                                T å R ò Ð i
```

In the context of encryption processes, when the final byte is extracted from each data block, it leads to varying outcomes depending on the mode of operation. Specifically, in the case of Output Feedback (OFB) and Cipher Feedback (CFB) modes, a portion of the information remains readable. However, when employing Electronic Codebook (ECB) or Cipher Block Chaining (CBC) modes, there is no readable information.

TASK 2.10

CBC mode is well-suited for applications where data confidentiality is a primary concern and deterministic encryption is not required. It is a popular choice for securing data in various contexts, including:

File or disk encryption: Protecting sensitive data stored on local disks or network-attached storage.

Secure communication over a network: Ensuring privacy and security in VPNs, TLS/SSL for secure web browsing, and secure email.

Data-at-rest encryption: Safeguarding data on databases, backups, or cloud storage.

Encrypted messaging applications: Securing real-time messaging and chat platforms.

ECB mode is rarely recommended for practical applications due to its vulnerability to repeated blocks and lack of security features. It should generally be avoided. However, in exceedingly rare situations, it may be appropriate when data confidentiality is not a primary concern, and deterministic encryption is required. Examples are limited and might include:

Storing publicly accessible, non-sensitive data that doesn't require strong encryption.

Data anonymization or pseudonymization scenarios where confidentiality isn't crucial, but deterministic transformations are desired.

TASK 2.11

Cipher Feedback (CFB):

CFB mode allows parallelization of encryption and decryption processes because it transforms plaintext or ciphertext one block at a time independently. Each block can be encrypted or decrypted separately, which makes it suitable for parallel processing.

CFB mode operates in a self-synchronizing manner, which means that a single block can be processed without needing the result of the previous block, facilitating parallelization.

Output Feedback (OFB):

OFB mode is another mode that allows for parallelization, as it encrypts and decrypts data block by block, independently of the previous blocks. It also operates in a self-synchronizing manner.

The independence of each block's encryption or decryption process makes it suitable for dividing the data into parts for parallel processing.