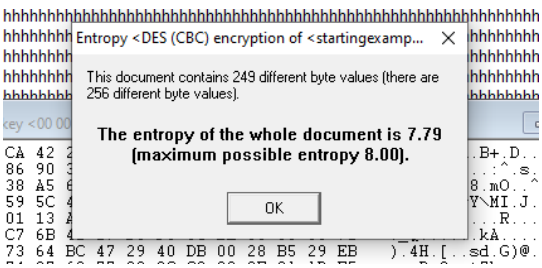
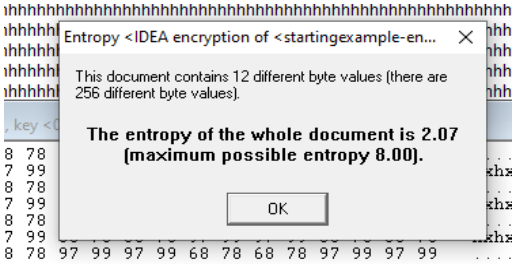
Block ciphers

Homogenius

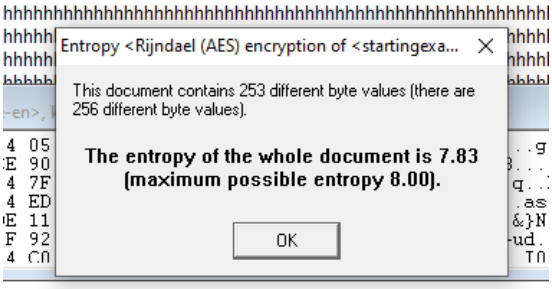
I put a thousand of “h” character in order to analysis entropy to find homogenius of the algorithms.



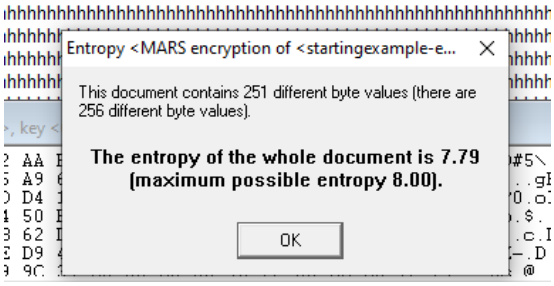
DES(CBC)



IDEA



AES(CBC)

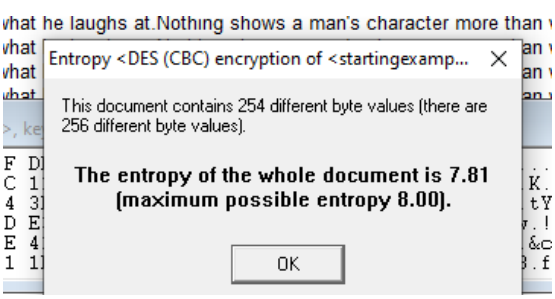


MARS

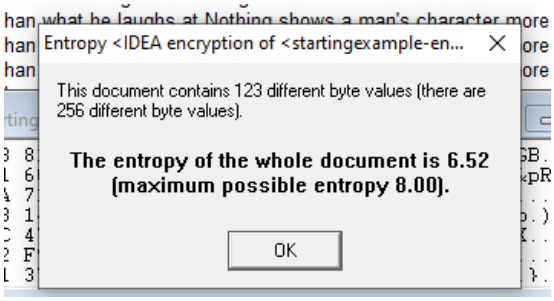
According to results, I see no such difference between the entropies of the document in algorithms except IDEA algorithm.

Medium-diversified

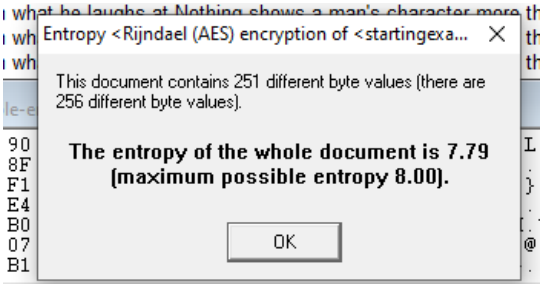
The repeated strings of my characters (totally 1020 character) are: ”Nothing shows a man's character more than what he laughs at.” That I used with algorithms in order to find medium-diversied of the algorithm.



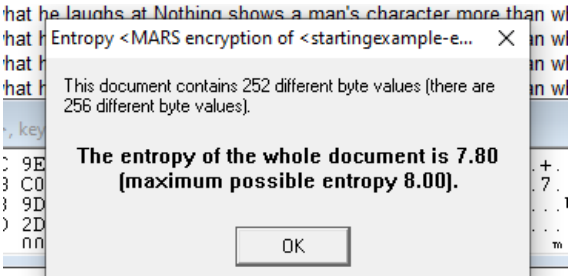
DES(CBC)



İDEA



AES(CBC)

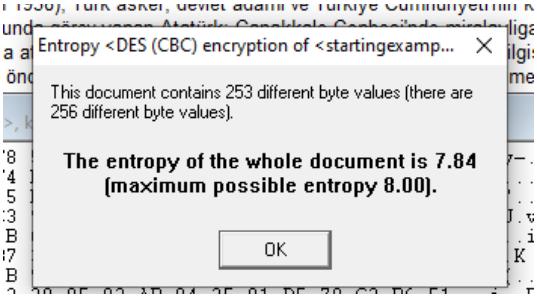


MARS

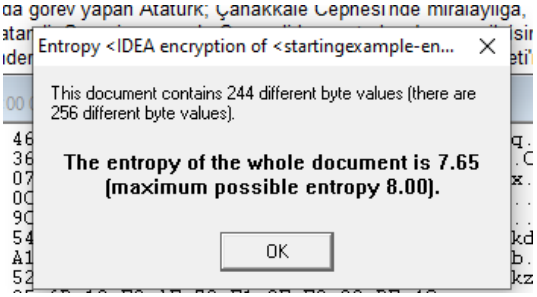
According to results, I see only maximum 0.3- 0.4 changes in the entropy of the documents. However, IDEA algorithm had some changes.

Highly-diversified

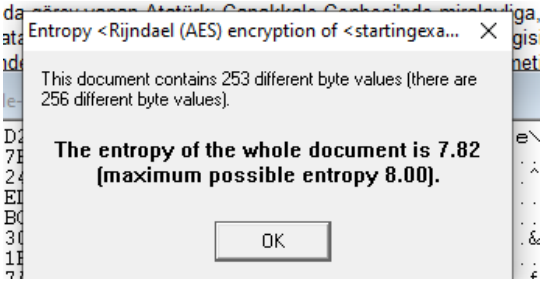
I used article copied from Wikipedia which has 1005 different character.



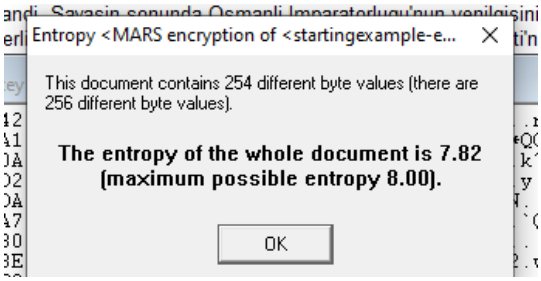
DES(CBC)



IDEA



AES(CBC)



MARS

At this part I come across with same result in AES and MARS algorithm. Furthermore, IDEA algorithm had similar result with other algorithms at this time.

The final table according to results.

Algorithms	Maximum Possible entropy	homogenius	Medium-diversified	Highly-diversified
DES(CBC)	8.00	7.79	7.81	7.84
IDEA	8.00	2.07	6.52	7.65
AES(CBC)	8.00	7.83	7.79	7.82
MARS	8.00	7.79	7.80	7.82

II. Questions:

1. Which algorithms are most popular?

AES. The Advanced Encryption Standard (AES) is the algorithm trusted as the standard by the U.S. Government and numerous organizations. And then twofish, idea, tripleDES.

2. Which parameter values (block length, key length) are nowadays considered standard(safe)?

Algorithms has different bits. The block size has a maximum of 256 bits, but the key size has no theoretical maximum. If a key is n bits long, then there are two to the nth power (2n) possible keys.

3. What can we say about the observed changes in histograms and entropy values during the realization of points 1 and 2?

I can see that the histogram and entropy values are changing. Some algorithms have approximately identical entropy values, and the maximum entropy values can be seen. Furthermore, the variance is getting more noticeable, despite the fact that it remains constant after a high. It implies that algorithms operate beautifully up to a point before failing to have a substantial impact.

4. Does the length of the block affect the entropy of the ciphertext?

To split data for encryption techniques, blocks are used. As a result, adding or removing blocks will have an immediate impact on the entropy values. It's difficult to say how much it will change, but it will have an effect eventually.

5. Does the length of the key influence the entropy of the ciphertext?

Key defines the strength of a key. A short key length means poor security. However, a long key length does not necessarily mean good security. The key length determines the maximum number of combinations required to break an encryption algorithm. If a key is n bits long, then there are two to the nth power (2^n) possible keys.

6. Does the observed entropy of a ciphertext depend on the entropy of pain text?

Entropy of a ciphertext affected only for IDEA algorithm according to my table. And rest of it almost same and there is no such differences between the algorithms. So that I think plaintext not that important.

7. **Does the observed ciphertext entropy depend on the algorithm used ?**

According to my observations via result on the table, in my opinion used algorithms are more critical in this situation. Plaintext does not affect as algorithm as do.

II. Questions:

1. **What do a ciphertext and its entropy look like for plain text with the homogeneous structure depending on the chosen encryption mode?**

We can see a distinct change in entropy between ciphertext and plaintext according to given text. It makes no difference whether the plaintext is homogeneous or not after the chosen encryption mode.

2. **What is the impact of errors introduced into the ciphertext after decryption, what does the plain text with changed one bit and multiple bits look like?**

unusual among public-key cryptosystems in that, with standard parameters, validly generated ciphertexts can fail to decrypt.

Every character texted in the plain text is increased the bits. So adding to plaintext might probably affect the plaintext as probably deleting does. Removing bit doesn't mean that all the plaintext has changed, it just deletes the text.

3. **What does each mode of operation do with the loss of the ciphertext?İs it possible to retrieve plain text after removing some parts from the ciphertext?**

We are right to retrieve plaintext of a ciphertext after the removing. If the removed part is a bit than it doesn't make such distinct change to decrypt. How removed part is bigger than the decryption became more complex. it depends.

The Cipher Feedback (CFB) mode makes a block cipher into a self-synchronizing stream cipher. If part of the ciphertext is lost then the receiver will lose only some part of the original message and should be able to continue

to correctly decrypt the rest of the blocks after processing some amount of input data. Only if a whole block size of ciphertext is lost CFB will synchronize but losing only a single byte or bit will permanently throw off decryption.

4. **Which of the modes of operation allows for encryption and decryption processes in parallel? Which mode of operation allows us to divide plaintext/ ciphertext into several parts to perform encryption or decryption independently (on different threads)?**

According to my research, we can decrypt the data in parallel, but it is not possible when encrypting data except Block cipher. Because, if a plaintext or ciphertext block is broken than it will affect all following block.

ECB - Parallel encryption of blocks of bits is possible, thus it is a faster way of encryption. Simple way of the block cipher.