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:

A screenshot of a computer

Description automatically generated

A screenshot of a computer screen

Description automatically generated

A screenshot of a computer

Description automatically generated

A screen shot of a graph

Description automatically generated

A screenshot of a graph

Description automatically generated

A screenshot of a graph

Description automatically generated

Medium-diversified text:

A screen shot of a graph

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer screen

Description automatically generated

A screenshot of a graph

Description automatically generated

A screenshot of a computer

Description automatically generated

Highly-diversified text:

A screenshot of a graph

Description automatically generated

A screen shot of a graph

Description automatically generated

A screenshot of a computer screen

Description automatically generated

A screenshot of a graph

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer screen

Description automatically generated

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

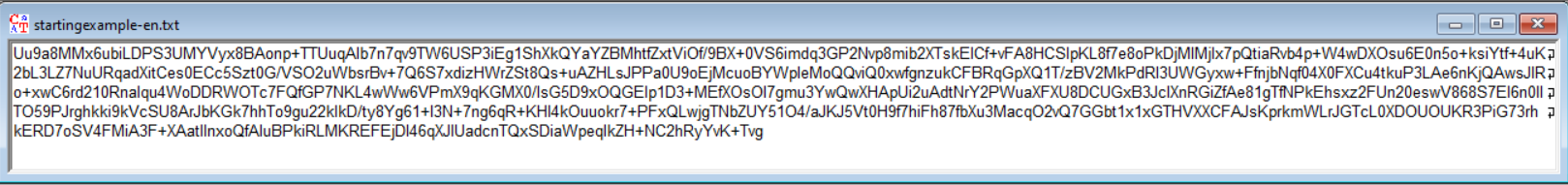
Key: 2164239413FCDB4209F24028CCFAE0FB

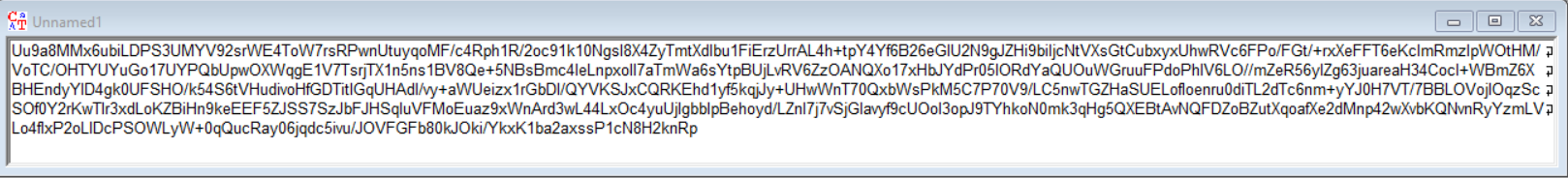
Plaintext:

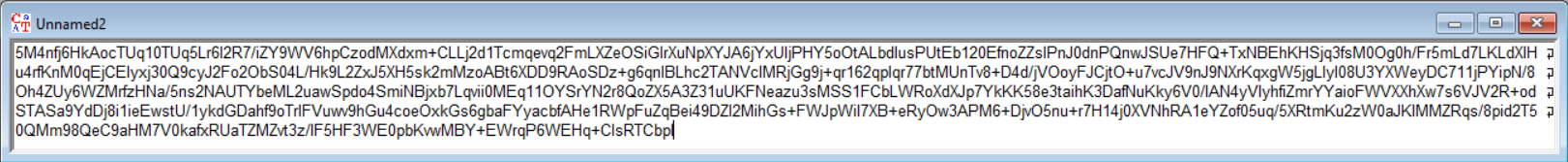
Entropy: 4.09  
A screenshot of a computer screen

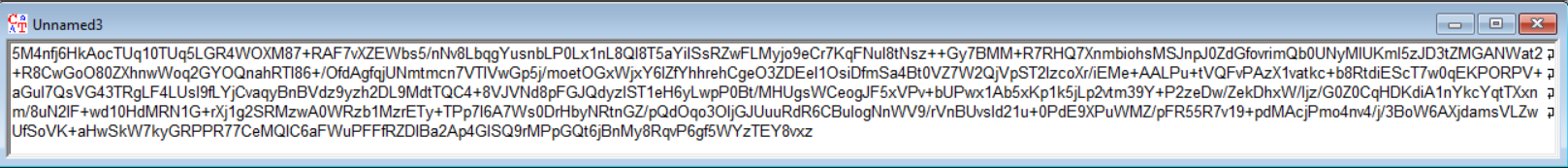
Description automatically generated

CBC:



ECB:  


OFB:  


CFB:  


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

CBC:

A screen shot of a graph

Description automatically generated

ECB:

A screenshot of a graph

Description automatically generated

OFB:

A screenshot of a graph

Description automatically generated

CFB:

A graph on a computer screen

Description automatically generated

TASK 2.4

abcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcdabcd

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

AES(CBC):

A screenshot of a graph

Description automatically generated

AES(CFB):  
A graph with lines on it

Description automatically generated with medium confidence

AES(ECB):  
A graph on a computer screen

Description automatically generated

AES(OFB):  
A screenshot of a graph

Description automatically generated

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:**  
A screenshot of a text

Description automatically generated

**Removing one byte:**  
A text on a page

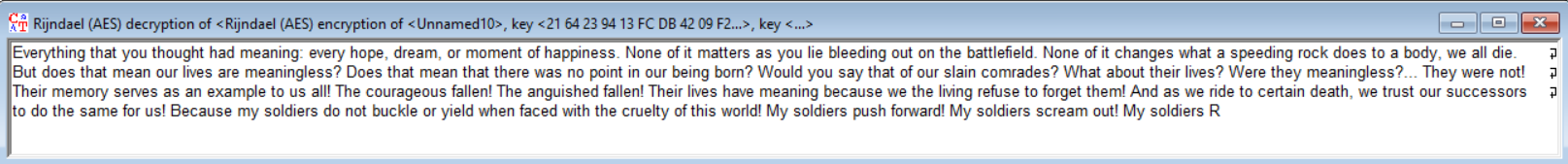
Description automatically generated

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

A text on a page

Description automatically generated

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



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)

A screenshot of a computer

Description automatically generated

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

Vvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvv

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

A screenshot of a computer

Description automatically generated

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):  
**A grid of numbers on a white background

Description automatically generated**AES(ECB):

A grid of numbers on a white background

Description automatically generated

AES(CBC)

A grid of numbers on a white background

Description automatically generated

AES(OFB):  
  
A grid of numbers on a white background

Description automatically generated

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.