2022

TEACHNOOK

(CYBER SECURITY)

MINI PROJECT

Presented by:-

Nitanshi Agarwal

9/1/2022

Content of your Project:-

Make a Report on Different Types of Ciphers With Examples And Screenshots of the Implementation.

INDEX

What is Cryptography?

Cryptography is technique of securing information and communications through use of codes so that only those person for whom the information is intended can understand it and process it. Thus preventing unauthorized access to information. The prefix “crypt” means “hidden” and suffix graphy means “writing”. In Cryptography the techniques which are use to protect information are obtained from mathematical concepts and a set of rule based calculations known as algorithms to convert messages in ways that make it hard to decode it. These algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on internet and to protect confidential transactions such as credit card and debit card transactions.

Techniques used For Cryptography: In today’s age of computers cryptography is often associated with the process where an ordinary plain text is converted to cipher text which is the text made such that intended receiver of the text can only decode it and hence this process is known as encryption. The process of conversion of cipher text to plain text this is known as decryption.

Features Of Cryptography are as follows:

1. **Confidentiality:** Information can only be accessed by the person for whom it is intended and no other person except him can access it.
2. **Integrity:** Information cannot be modified in storage or transition between sender and intended receiver without any addition to information being detected.

3. **Non-repudiation:** The creator/sender of information cannot deny his intention to send information at later stage.
4. **Authentication:** The identities of sender and receiver are confirmed. As well as destination/origin of information is confirmed.

Types Of Cryptography: In general there are three types Of cryptography:

1. **Symmetric Key Cryptography:** It is an encryption system where the sender and receiver of message use a single common key to encrypt and decrypt messages. Symmetric Key Systems are faster and simpler but the problem is that sender and receiver have to somehow exchange key in a secure manner. The most popular symmetric key cryptography system is Data Encryption System(DES).
2. **Hash Functions:** There is no usage of any key in this algorithm. A hash value with fixed length is calculated as per the plain text which makes it impossible for contents of plain text to be recovered. Many operating systems use hash functions to encrypt passwords.
3. **Asymmetric Key Cryptography:** Under this system a pair of keys is used to encrypt and decrypt information. A public key is used for encryption and a private key is used for decryption. Public key and Private Key are different. Even if the public key is known by everyone the intended receiver can only decode it because he alone knows the private key.

What is Cipher Text?

Ciphertext is encrypted text transformed from plaintext using an encryption algorithm. Ciphertext can't be read until it has been converted into plaintext (decrypted) with a key. The decryption cipher is an algorithm that transforms the ciphertext back into plaintext.

- ## Uses of ciphertext

Symmetric ciphers, which are typically used to secure online communications, are incorporated into many different network protocols to be used to encrypt exchanges. For example, Transport Layer Security uses ciphers to encrypt application layer data.

Virtual private networks connecting remote workers or remote branches into corporate networks use protocols with symmetric ciphers to protect data communications. Symmetric ciphers protect data privacy in most Wi-Fi networks, online banking, e-commerce services and mobile telephony.

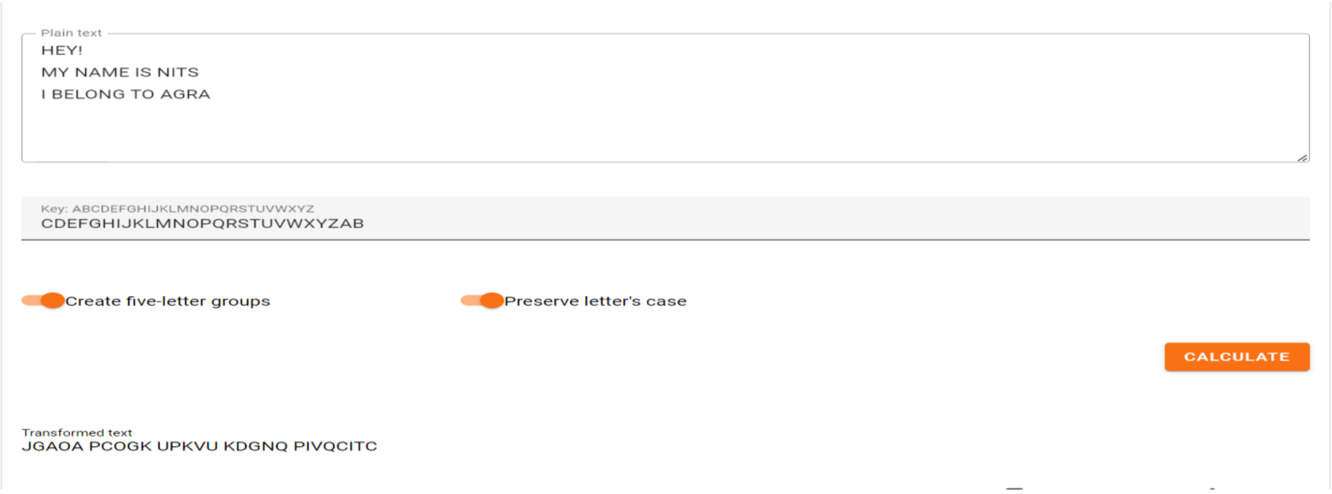
Other protocols, including secure shell, OpenPGP and Secure/Multipurpose Internet Mail Extensions use asymmetric cryptography to encrypt and authenticate endpoints but also to securely exchange the symmetric keys to encrypt session data. For performance reasons, protocols often rely on ciphers to encrypt session data.

Different Types Of Cipher Text

1-SUBSTITUTION CIPHER

Replace bits, characters, or character blocks in plaintext with alternate bits, characters or character blocks to produce ciphertext. A substitution cipher may be monoalphabetic or polyalphabetic*:*

- A single alphabet is used to encrypt the entire plaintext message. For example, if the letter A is enciphered as the letter K, this will be the same for the entire message.
- A more complex substitution using a mixed alphabet to encrypt each bit, character or character block of a plaintext message. For instance, the letter A may be encoded as the letter K for part of the message, but later it might be encoded as the letter W.



Plain text
HEY!
MY NAME IS NITS
I BELONG TO AGRA

Key: ABCDEFGHIJKLMNOPQRSTUVWXYZ
CDEFGHIJKLMNOPQRSTUVWXYZAB

● Create five-letter groups

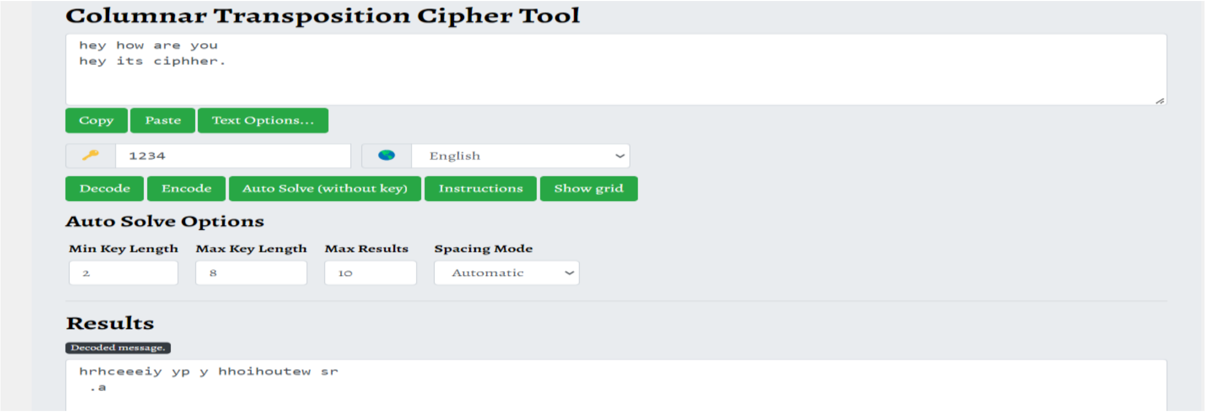
● Preserve letter's case

Transformed text
JGAOA PCOGK UPKVU KDGNQ PIVQCITC

2-TRANSPOSITION CIPHER

Unlike substitution ciphers that replace letters with other letters, transposition ciphers keep the letters the same, but rearrange their order according to a specific algorithm. For instance, in a simple columnar transposition cipher, a message might be read the ciphertext.

DECODE



```
hey how are you
hey its ciphher.
```

Key: 1234

Language: English

Min Key Length: 2

Max Key Length: 8

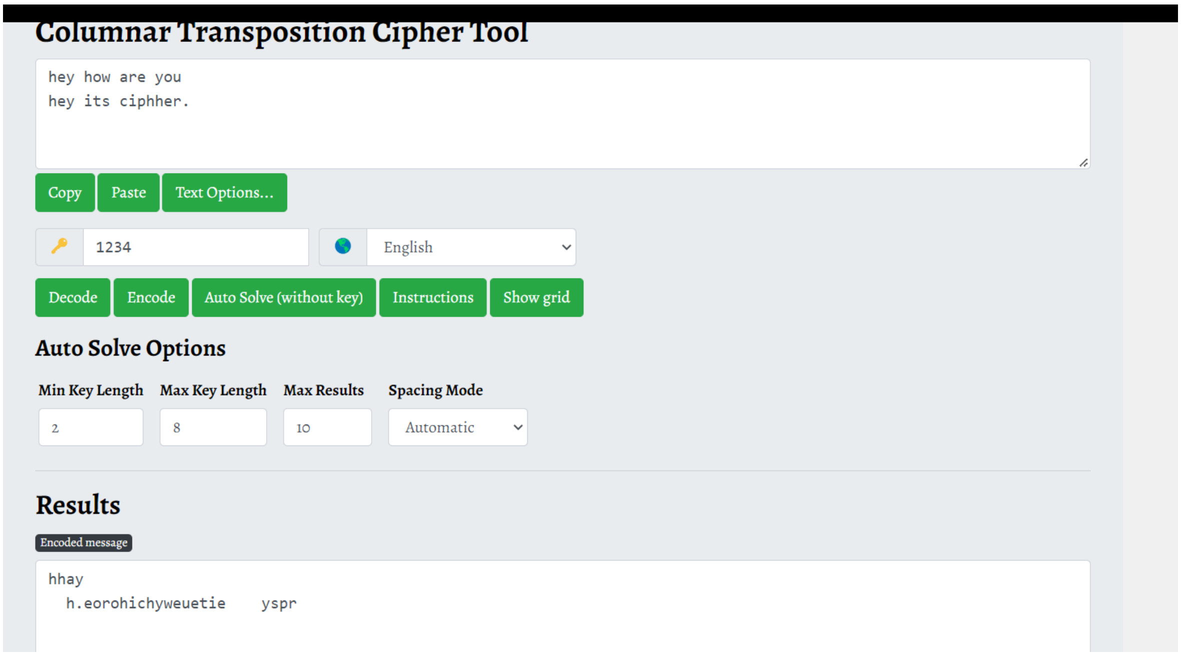
Max Results: 10

Spacing Mode: Automatic

Decoded message.

```
hrhceeeiy yp y hhoihoutew sr
 .a
```

ENCODE



```
hey how are you
hey its ciphher.
```

Key: 1234

Language: English

Min Key Length: 2

Max Key Length: 8

Max Results: 10

Spacing Mode: Automatic

Encoded message

```
hhay
  h.eorohichyweuetie    yspr
```

3-BLOCK CIPHER:-

A **block cipher** is a ***symmetric cryptographic technique*** which we used to ***encrypt a fixed-size data block using a shared, secret key.*** During **encryption,** we used ***plaintext*** and **ciphertext** is the resultant encrypted text. It uses the same key to encrypt both the ***plaintext,*** and the ***ciphertext.*** A **block cipher** processes the data blocks of fixed size. Typically, a message's size exceeds a block's size. As a result, the lengthy message is broken up into a number of sequential message blocks, and the cipher operates on these blocks one at a time.

AES Encryption

AES is a block cipher.
The key size can be 128/192/256 bits.Encrypts data in blocks of 128 bits each. That means it takes 128 bits as input and outputs 128 bits of encrypted cipher text as output. AES relies on substitution-permutation network principle which means it is performed using a series of linked operations which involves replacing and shuffling of the input data.

DES Encryption

Data encryption standard (DES) has been found vulnerable to very powerful attacks and therefore, the popularity of DES has been found slightly on the decline. DES is a block cipher and encrypts data in blocks of size of **64 bits** each, which means 64 bits of plain text go as the input to DES, which produces 64 bits of ciphertext. The same algorithm and key are used for encryption and decryption, with minor differences. The key length is **56 bits**.

Different Modes of AES Encryption

AES offers 2 different modes of encryption - ECB and CBC modes.

- ECB(Electronic Code Book) is the simplest encryption mode and does not require IV for encryption. The input plain text will be divided into blocks and each block will be encrypted with the key provided and hence identical plain text blocks are encrypted into identical cipher text blocks.
- CBC(Cipher Block Chaining) mode is highly recommended, and it is an advanced form of block cipher encryption. It requires IV to make each message unique meaning the identical plain text blocks are encrypted into dissimilar cipher text blocks. Hence, it provides more robust encryption as compared to ECB mode, but it is a bit slower as compared to ECB mode. If no IV is entered then default will be used here for CBC mode and that defaults to a zero based byte[16].

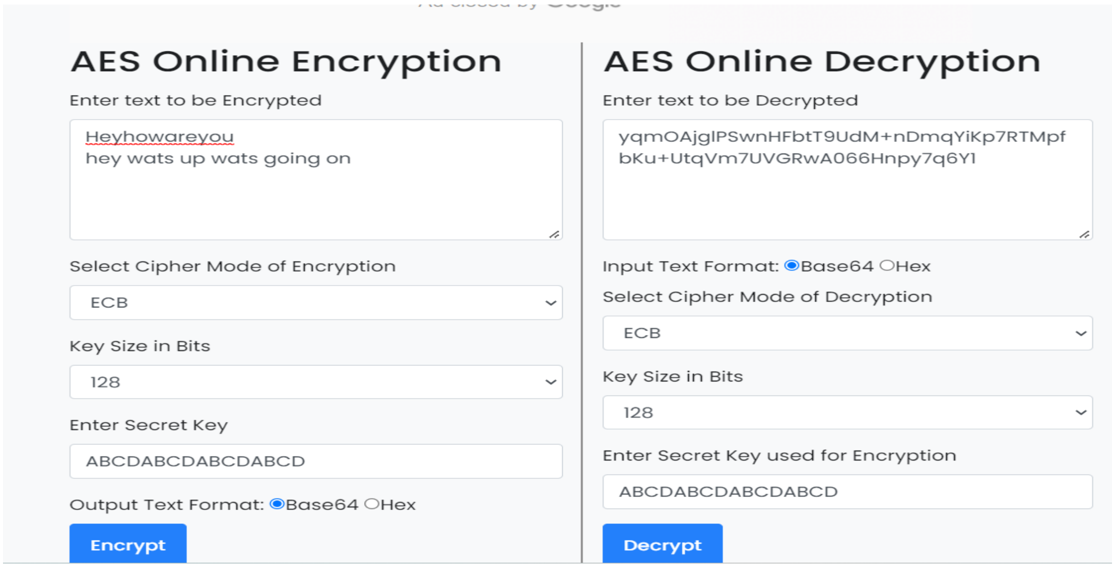
Different Modes of DES Encryption

Data Encryption Standard or DES - it is one of the key player in the history of modern cryptography, as it was a major agent-of-change that brought a revolution in the world of symmetric cryptography after its publication in 1977. . We will discuss mainly two modes here: ECB (Electronic CodeBook Mode) and the CBC (Cipher Block Chaining) mode. We have already a long binary string or data which is to be encrypted, and we try to encrypt the entire data. Our obvious step in block cipher is to 'decompose' / divide entire data into different blocks (each block having 64 bits as in DES). If the entire data is exactly divisible into blocks, then it's ok; otherwise, we 'pad' the data using various schemes.

ECB(base64)

This mode of operation is the simplest of all. The plaintext is divided into blocks with a size of 128 bits. Then each block is encrypted with the same key and algorithm. Therefore, it produces the same result for the same block. This is the main weakness of this mode, and **it's not recommended for encryption**. It requires padding data.

Input:



AES Online Encryption

Enter text to be Encrypted

```
Heyhowareyou
hey wats up wats going on
```

Select Cipher Mode of Encryption: ECB

Key Size in Bits: 128

Enter Secret Key: ABCDABCDABCDABCD

Output Text Format: ● Base64 ○ Hex

Encrypt

AES Online Decryption

Enter text to be Decrypted

```
yqmOAjglPSwnHFbtT9UdM+nDmqYiKp7RTMpf
bKu+UtqVm7UVGRwA066Hnpy7q6Y1
```

Input Text Format: ● Base64 ○ Hex

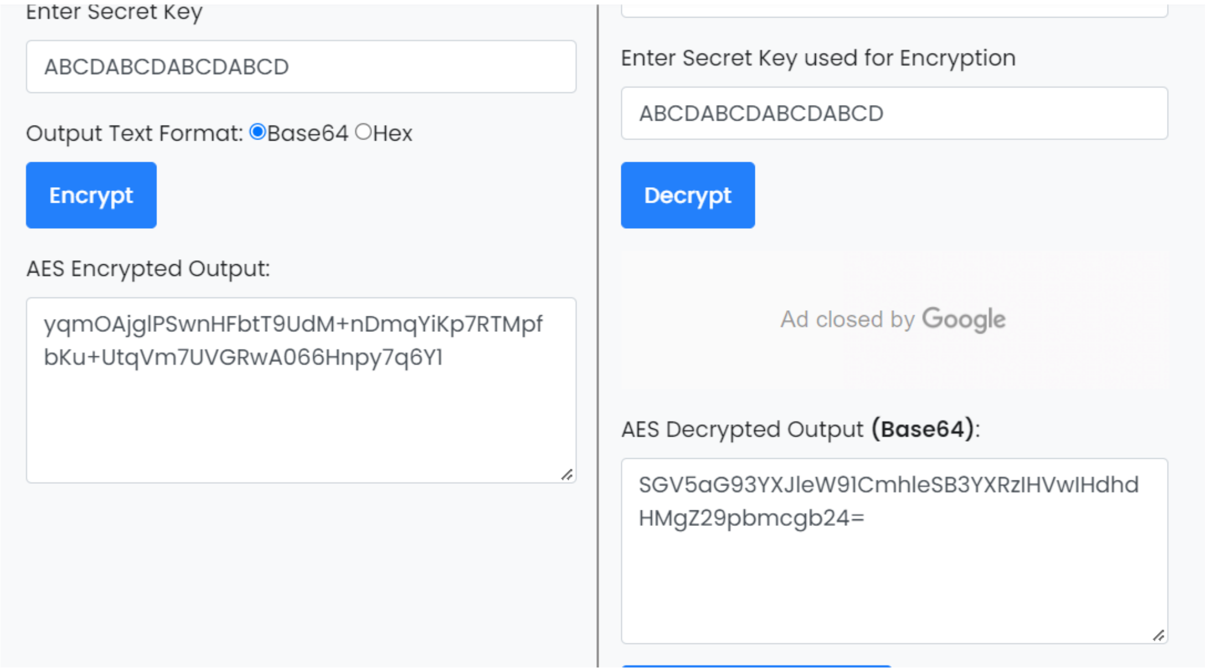
Select Cipher Mode of Decryption: ECB

Key Size in Bits: 128

Enter Secret Key used for Encryption: ABCDABCDABCDABCD

Decrypt

Output:



Enter Secret Key: ABCDABCDABCDABCD

Output Text Format: ● Base64 ○ Hex

Encrypt

AES Encrypted Output:

```
yqmOAjglPSwnHFbtT9UdM+nDmqYiKp7RTMpf
bKu+UtqVm7UVGRwA066Hnpy7q6Y1
```

Enter Secret Key used for Encryption: ABCDABCDABCDABCD

Decrypt

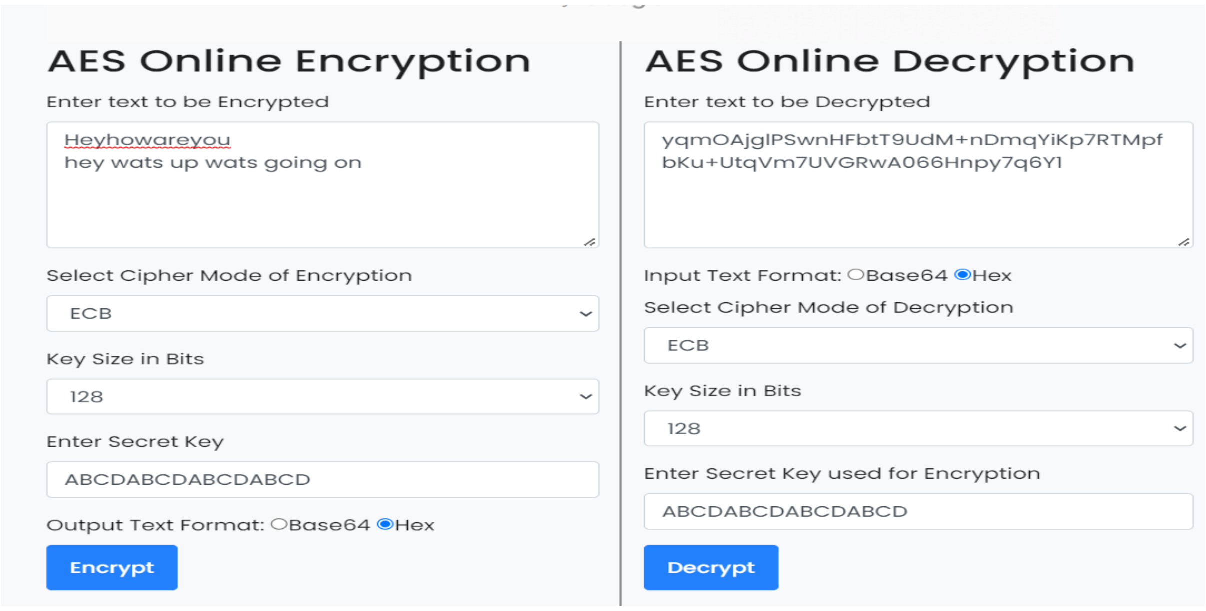
Ad closed by Google

AES Decrypted Output **(Base64)**:

```
SGV5aG93YXJleW91CmhleSB3YXRzIHVwIHdhd
HMgZ29pbmcgb24=
```

ECB(hexadecimal)

Input:



Enter text to be Encrypted

Heyhowareyou
hey wats up wats going on

Select Cipher Mode of Encryption: ECB

Key Size in Bits: 128

Enter Secret Key: ABCDABCDABCDABCD

Output Text Format: ○Base64 ●Hex

Enter text to be Decrypted

yqmOAjglPSwnHFbtT9UdM+nDmqYiKp7RTMpf
bKu+UtqVm7UVGRwA066Hnpy7q6Y1

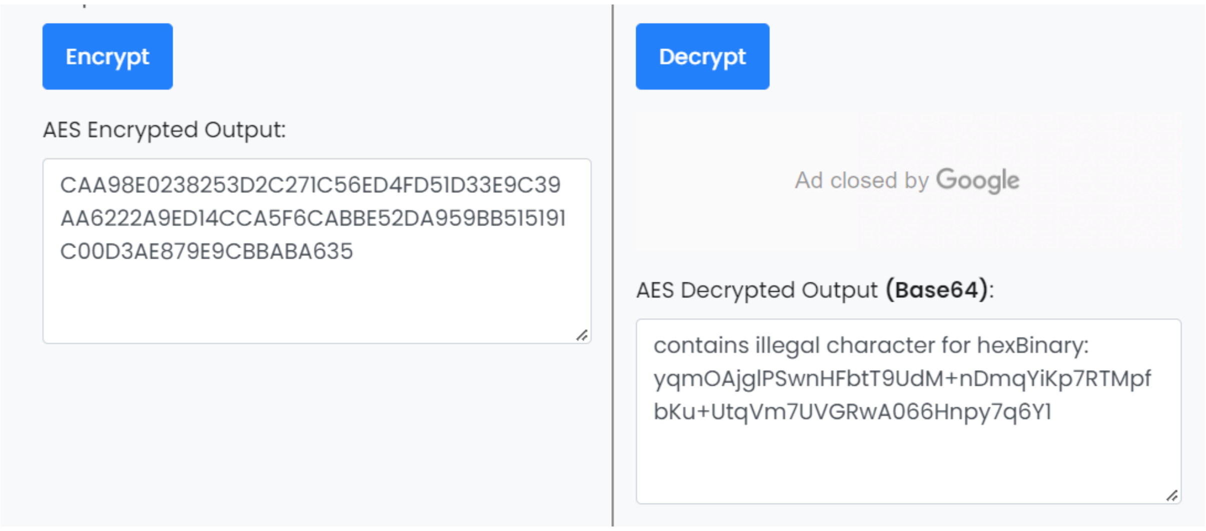
Input Text Format: ○Base64 ●Hex

Select Cipher Mode of Decryption: ECB

Key Size in Bits: 128

Enter Secret Key used for Encryption: ABCDABCDABCDABCD

Output:



AES Encrypted Output:

```
CAA98E0238253D2C271C56ED4FD51D33E9C39
AA6222A9ED14CCA5F6CABBE52DA959BB515191
C00D3AE879E9CBBABA635
```

AES Decrypted Output **(Base64)**:

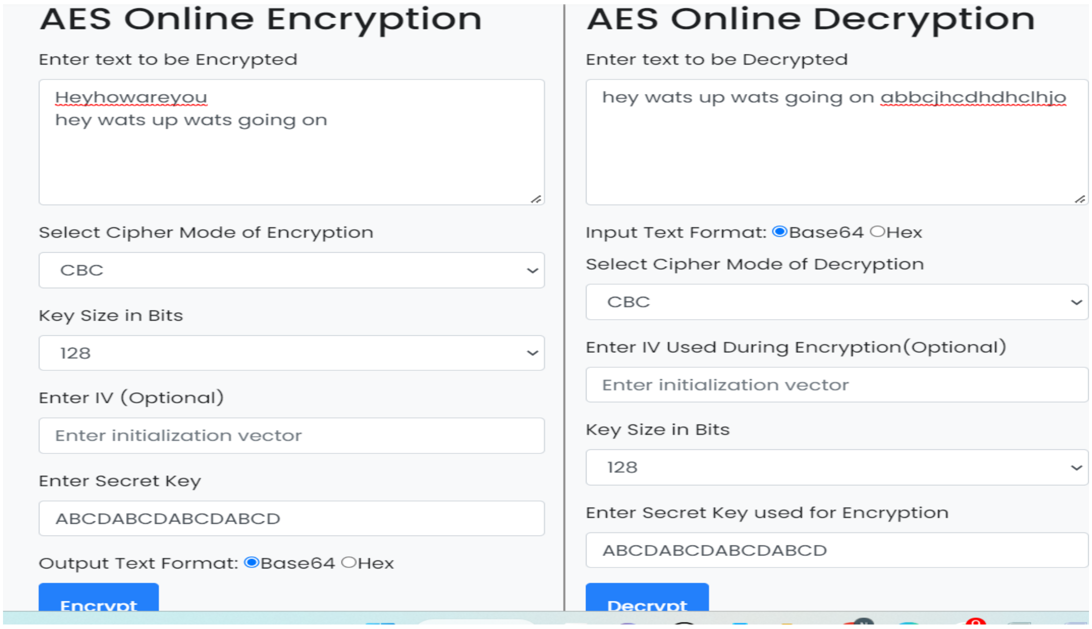
```
contains illegal character for hexBinary:
yqmOAjglPSwnHFbtT9UdM+nDmqYiKp7RTMpf
bKu+UtqVm7UVGRwA066Hnpy7q6Y1
```

CBC(base64)

In order to overcome the ECB weakness, CBC mode uses an Initialization Vector (IV) to augment the encryption. First, CBC uses the plaintext block xor with the IV. Then it encrypts the result to the ciphertext block. In the next block, it uses the encryption result to xor with the plaintext block until the last block.

In this mode, encryption can't be parallelized, but decryption can be parallelized. It also requires padding data.

Input:



AES Online Encryption

Enter text to be Encrypted

Heyhowareyou
hey wats up wats going on

Select Cipher Mode of Encryption

CBC

Key Size in Bits

128

Enter IV (Optional)

Enter initialization vector

Enter Secret Key

ABCDABCDABCDABCD

Output Text Format: ● Base64 ○ Hex

AES Online Decryption

Enter text to be Decrypted

hey wats up wats going on abbcjhcdhdhclhjo

Input Text Format: ● Base64 ○ Hex

Select Cipher Mode of Decryption

CBC

Enter IV Used During Encryption(Optional)

Enter initialization vector

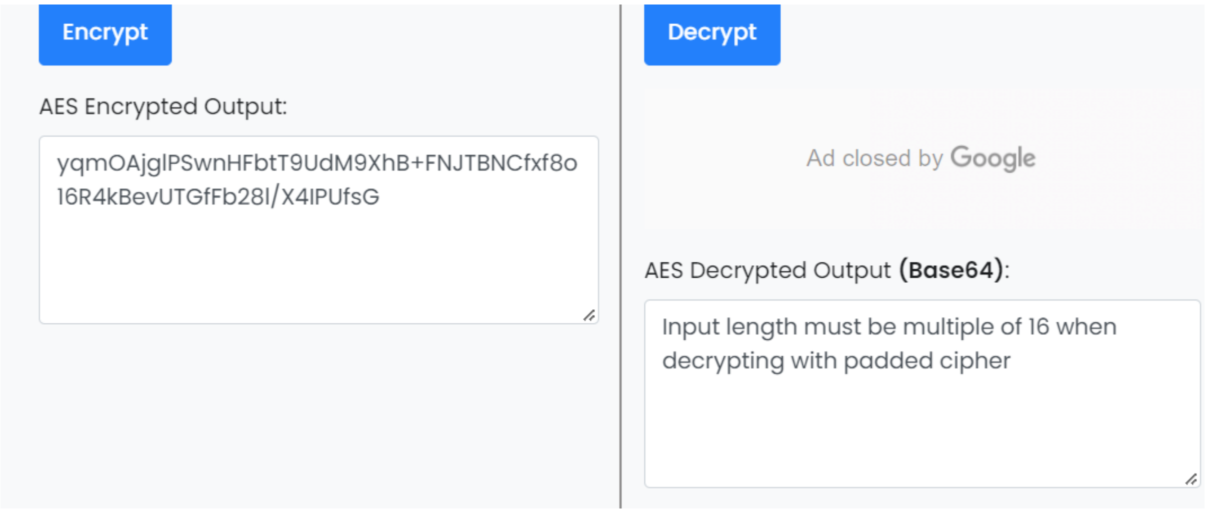
Key Size in Bits

128

Enter Secret Key used for Encryption

ABCDABCDABCDABCD

Output:



AES Encrypted Output:

yqmOAjgIPSwnHFbtT9UdM9XhB+FNJTBNCfxf8o16R4kBevUTGfFb28I/X4IPUfsG

AES Decrypted Output **(Base64)**:

Input length must be multiple of 16 when decrypting with padded cipher

4.STREAM CIPHER:-

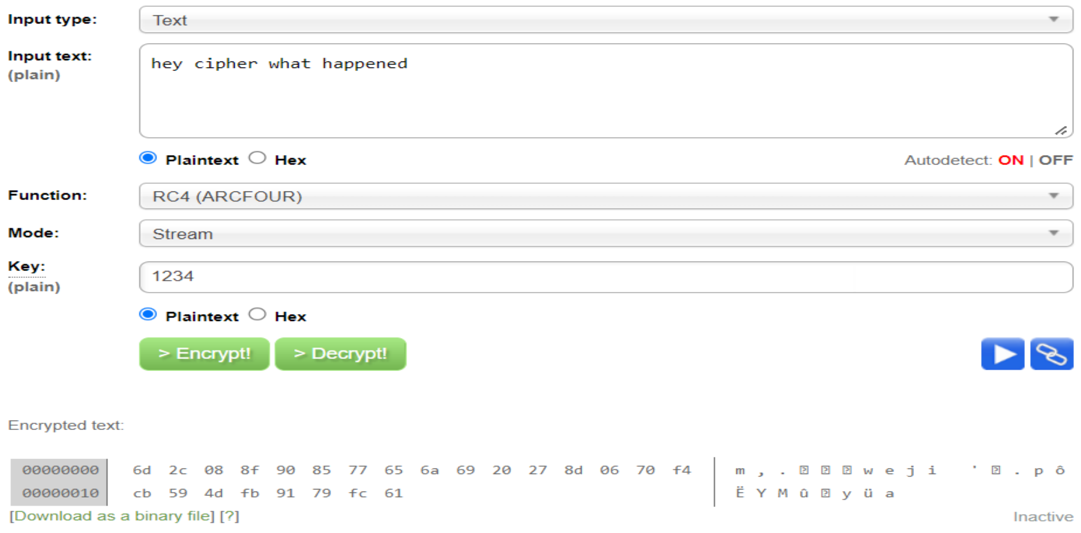
In stream cipher, one byte is encrypted at a time while in block cipher ~128 bits are encrypted at a time.

Initially, a key(k) will be supplied as input to pseudorandom bit generator and then it produces a random 8-bit output which is treated as keystream.

The resulted keystream will be of size 1 byte, i.e., 8 bits.

1. Stream Cipher follows the sequence of pseudorandom number stream.
2. One of the benefits of following stream cipher is to make cryptanalysis more difficult, so the number of bits chosen in the Keystream must be long in order to make cryptanalysis more difficult.
3. By making the key more longer it is also safe against brute force attacks.
4. The longer the key the stronger security is achieved, preventing any attack.
5. Keystream can be designed more efficiently by including more number of 1s and 0s, for making cryptanalysis more difficult.
6. Considerable benefit of a stream cipher is, it requires few lines of code compared to block cipher.

Encode(plaintext-plaintext)



Input type: Text

Input text: (plain) hey cipher what happened

● Plaintext ○ Hex

Autodetect: ON | OFF

Function: RC4 (ARCFOUR)

Mode: Stream

Key: (plain) 1234

● Plaintext ○ Hex

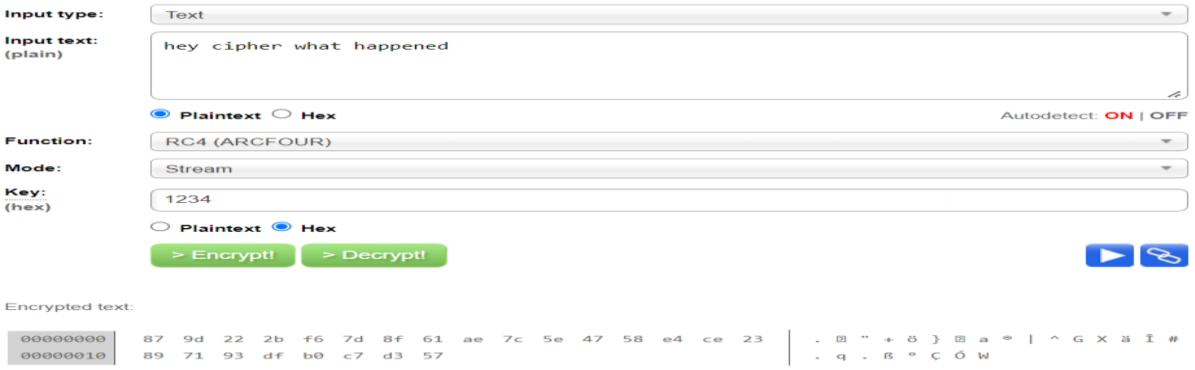
Encrypted text:

```
00000000   6d 2c 08 8f 90 85 77 65 6a 69 20 27 8d 06 70 f4 | m , . ⍰ ⍰ ⍰ w e j i   ' ⍰ . p ô
00000010   cb 59 4d fb 91 79 fc 61                         | Ë Y M û ⍰ y ü a
```

[Download as a binary file] [?]

Inactive

Encode(plaintext-hex)



Input type: Text

Input text: (plain) hey cipher what happened

● Plaintext ○ Hex

Function: RC4 (ARCFOUR)

Mode: Stream

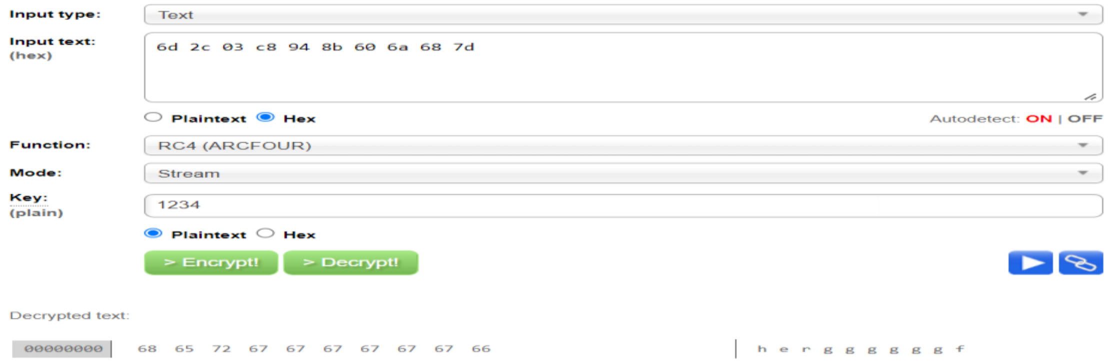
Key: (hex) 1234

○ Plaintext ● Hex

Encrypted text:

```
00000000  87 9d 22 2b f6 7d 8f 61 ae 7c 5e 47 58 e4 ce 23 | . ⊠ " + ö } ⊠ a ° | ^ G X ä Î #
00000010  89 71 93 df b0 c7 d3 57                         | . q . ß ° Ç Ó W
```

Decode



Input type: Text

Input text: (hex) 6d 2c 03 c8 94 8b 60 6a 68 7d

○ Plaintext ● Hex

Function: RC4 (ARCFOUR)

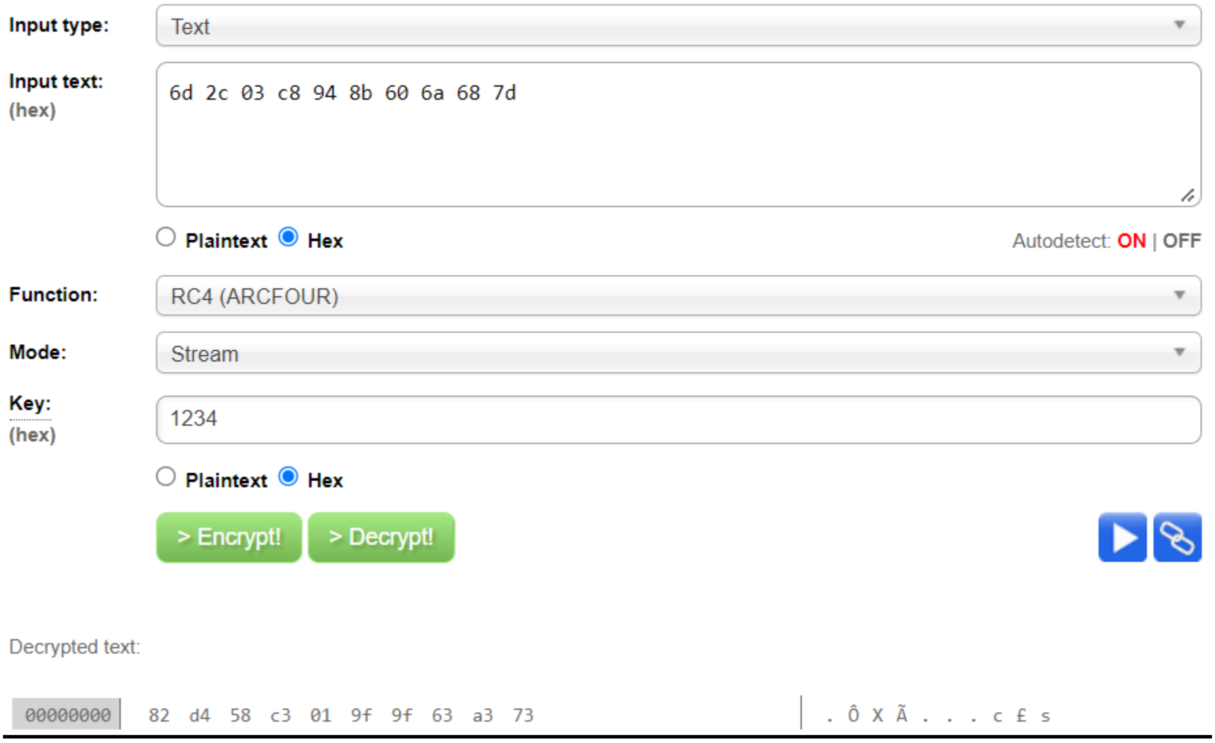
Mode: Stream

Key: (plain) 1234

● Plaintext ○ Hex

Decrypted text:

```
00000000  68 65 72 67 67 67 67 67 67 66 | h e r g g g g g g f
```



Input type: Text

Input text: (hex) 6d 2c 03 c8 94 8b 60 6a 68 7d

○ Plaintext ● Hex

Function: RC4 (ARCFOUR)

Mode: Stream

Key: (hex) 1234

○ Plaintext ● Hex

Decrypted text:

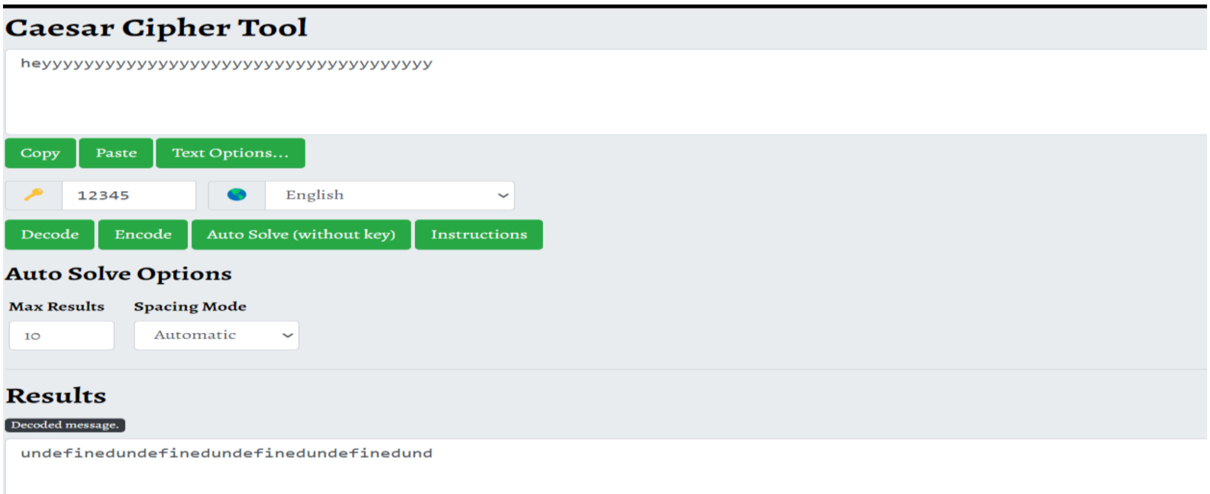
```
00000000  82 d4 58 c3 01 9f 9f 63 a3 73 | . Ô X Ã . . . c £ s
```

5.CAESER CIPHER:-

The Caesar Cipher technique is one of the earliest and simplest methods of encryption technique. It’s simply a type of substitution cipher, i.e., each letter of a given text is replaced by a letter with a fixed number of positions down the alphabet. For example with a shift of 1, A would be replaced by B, B would become C, and so on. The method is apparently named after Julius Caesar, who apparently used it to communicate with his officials.

Thus to cipher a given text we need an integer value, known as a shift which indicates the number of positions each letter of the text has been moved down.
The encryption can be represented using modular arithmetic by first transforming the letters into numbers, according to the scheme, A = 0, B = 1,…, Z = 25.

DECODE



Caesar Cipher Tool

heyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyy

🔑 12345 English

Auto Solve Options

Max Results 10

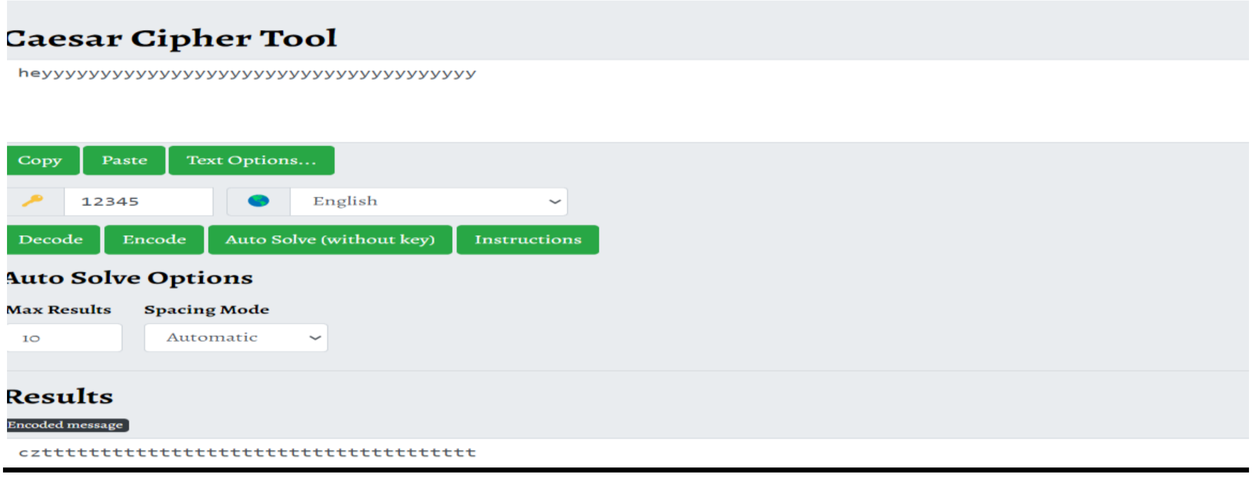
Spacing Mode Automatic

Results

Decoded message.

undefinedundefinedundefinedundefinedund

ENCODE



Caesar Cipher Tool

heyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyy

🔑 12345 English

Auto Solve Options

Max Results 10

Spacing Mode Automatic

Results

Encoded message

czpresentation

THANK

YOU!