**Encryption and Decryption**

Encryption is the process by which a readable message is converted to an unreadable form to prevent unauthorized parties from reading it**.**

Decryption is the process of converting an encrypted message back to its original (readable) format. The original message is called the plaintext message.

**Advanced Encryption Standard(AES) Algorithm**

AES is widely used today as it is a much stronger than DES and triple DES despite being harder to implement.

* AES is a block cipher.
* The key size can be 128/192/256 bits.
* Encrypts data in a block 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.

**Working:**

1. AES-128 uses a 128-bit key length to encrypt and decrypt a block of messages.
2. AES-192 uses a 192-bit key length to encrypt and decrypt a block of messages.
3. AES-256 uses a 256-bit key length to encrypt and decrypt a block of messages.

Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128, 192 and 256 bits, respectively. Symmetric, also known as [secret key](https://www.techtarget.com/searchsecurity/definition/private-key), ciphers use the same key for encrypting and decrypting. The sender and the receiver must both know -- and use -- the same secret key.

There are 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. A round consists of several processing steps that include substitution, transposition and mixing of the input [plaintext](https://www.techtarget.com/searchsecurity/definition/plaintext) to transform it into the final output of cipher text.

The AES encryption algorithm defines numerous transformations that are to be performed on data stored in an array. The first step of the cipher is to put the data into an array, after which the cipher transformations are repeated over multiple encryption rounds. The first transformation in the AES encryption cipher is substitution of data using a substitution table. The second transformation shifts data rows. The third mixes columns. The last transformation is performed on each column using a different part of the [encryption key](https://www.techtarget.com/searchsecurity/definition/key). Longer keys need more rounds to complete.

**Clap Command:**

Clap is a library that provides functionality to generate parsing logic for arguments, provides a neat and tidy CLI for applications, including an explanation of arguments and an –h help command.

Adding clap to a project:

To incorporate a clap into our project we have to add the dependencies clap = {version = “3.1.6”,features = [“derive”]}; inside the cargo.toml.

Clap has a subcommand feature that can provide apps with multiple subcommands. To use it, define another struct with its own arguments that will be the subcommand. The main argument struct contains the arguments struct contains the arguments common to all the subcommands, and then the subcommands.

Chacha20-poly1305:

The ChaCha20 stream cipher and the Poly1305 authenticator are cryptographic algorithms, having the aim of high security margins, while achieving high performance on a broad range of software platforms

References:

1. <https://docs.oracle.com/cd/E36784_01/html/E37124/scftask-4.html>
2. <https://kerkour.com/rust-file-encryption>
3. <https://www.youtube.com/watch?v=l0AmlU-4IRM>