1. Key - The key is a secret value that is used to encrypt and decrypt data. It must be a multiple of 128 bits (16 bytes) or 256 bits (32 bytes) in length, depending on the AES variant used. The key is usually generated randomly or derived from a password using a key derivation function.
2. Plaintext - The plaintext is the data that is to be encrypted. It can be any data in binary format, such as a file or a message.
3. Initialization Vector (IV) - The IV is a random value that is used to ensure that the same plaintext will produce different ciphertext every time it is encrypted with the same key. The IV is a 16-byte value for AES-128 and a 32-byte value for AES-256.

Optional parameters for AES encryption include:

1. Mode of Operation - AES can be used in various modes of operation to provide additional security, such as CBC (Cipher Block Chaining), CTR (Counter), or GCM (Galois/Counter Mode).
2. Padding - AES works on blocks of 128 bits, so if the plaintext is not a multiple of 128 bits, it must be padded to ensure that it can be encrypted. There are several padding schemes, such as PKCS#7 or ISO/IEC 7816-4.
3. Key Expansion - In order to generate the key schedule, the key is expanded into a larger set of round keys. The number of rounds depends on the key size and the block size, and it can be 10, 12, or 14 for AES-128, AES-192, and AES-256, respectively.
4. Salt - In some cases, a salt value may be used to add randomness to the key derivation process, making it more resistant to attacks.

Rot 47

ROT13 (rotate by 13 places) is a simple Caesar cipher technique that replaces each letter of the alphabet with the letter 13 places ahead of it in the alphabet. There is only one parameter required for ROT13 encryption:

1. Plaintext - The plaintext is the data that is to be encrypted. It can be any text in ASCII format, such as a message or a file.

To encrypt the plaintext using ROT13, simply replace each letter in the text with the letter 13 places ahead of it in the alphabet. For example, the letter "A" would be replaced with the letter "N", "B" with "O", and so on. When you reach the end of the alphabet, start again from the beginning (i.e. "Z" becomes "M", "Y" becomes "L", and so on).

It's important to note that ROT13 is a very weak encryption method and is not suitable for secure communication or data protection. It is primarily used for obfuscation or as a simple way to encode text in situations where a small amount of security is required.

Ui design

Inputs:

Password

File

Encryption type.

Outputs:

Password?

Plain text encrypted text.

Visual:

Dark mode “Hacker mode?”

Loading bar

File -> AES + XOR

Password -> Rot47