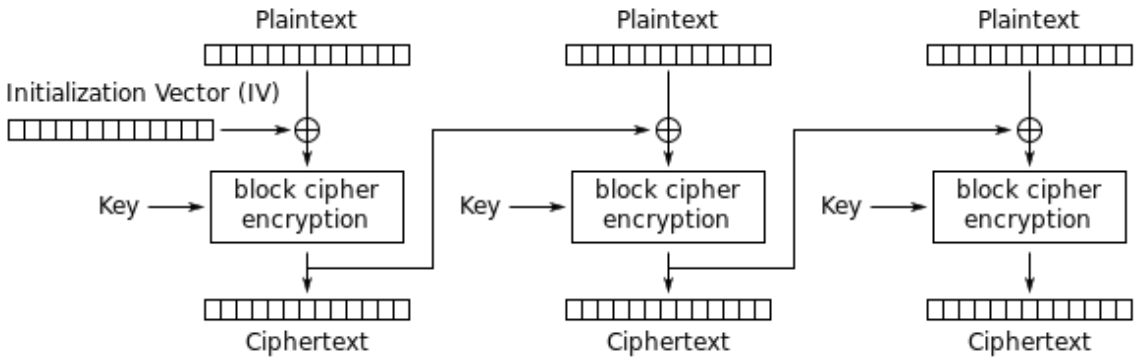
Explaination of encrypyt_classical.py

Major Highlights

- Encryption used is CBC(Cipher Block Chaining)
- In CBC, each block of plaintext is XORed with the previous ciphertext block before being encrypted,
  and then it is xored with the same key of size == Block size
- Zero Padding is used at the last block, if the plain text is not completely fit into Blocks, extra padding is used at the end.
- Initial Vector(IV) is used as passphrase.
- Block size used is 64 bits == 8 bytes == 8 CHARACTERS
- Key size is same as BLock Size == 64 bits

For more further study, read here



Cipher Block Chaining (CBC) mode encryption

Line by line explanation

- Line 8-9: import libraries
- Line 21-25: Reduce the passphrase to a bit array of size BLOCKSIZE
- LIne 28-33: Get key as user input
- Line 36-39: Reduce the key to a bit array of size BLOCKSIZE
- Line 45-54: Xoring the Blocks as follows
  C(i) = C(i-1) ^ P(i) ^ K, where i ∈ [0, NUMB_BLOCKS]
  For i = 0, C(i-1) is Initial Vector
- Line 57: Convert the Bitvector to a ascii charater string
- Line 60-62: Save the obtained cipher text to file.