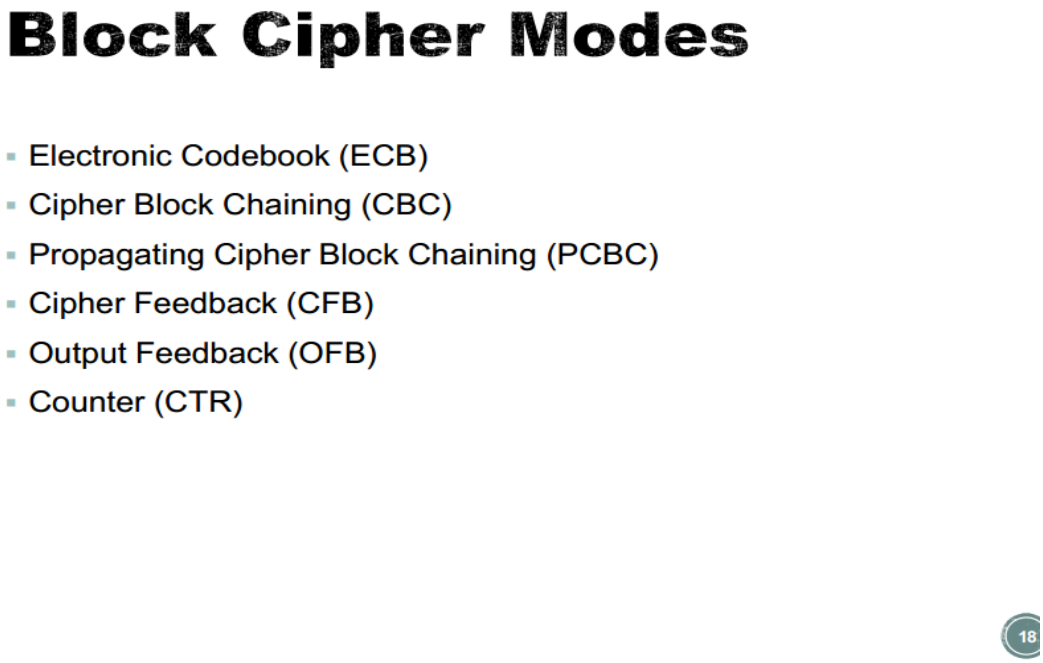
ECB Vs Cipher Block Chaining

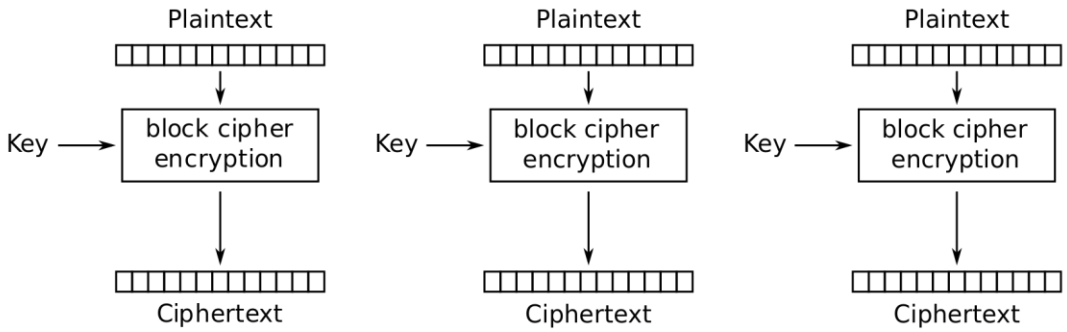


ECB (Electronic Codebook)

AES ECB is a notoriously bad method of encrypting bmp images because it keeps encrypting the blocks the same way throughout the image.

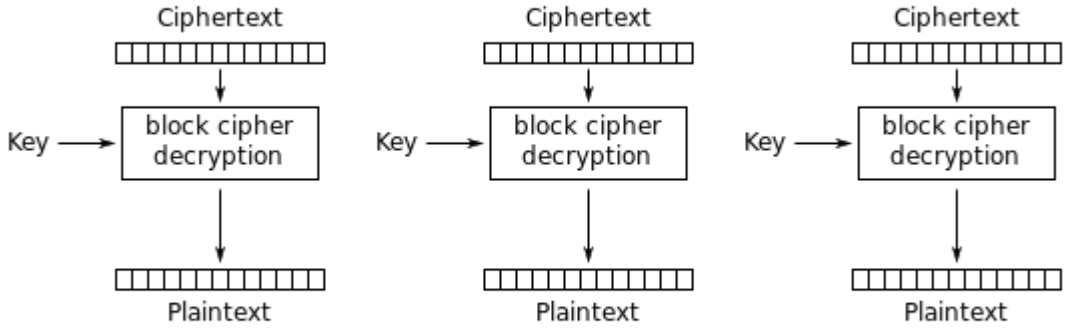
https://pthree.org/2012/02/17/ecb-vs-cbc-encryption/

https://www.rogdham.net/2012/11/24/ecb-youre-doing-it-wrong.en https://doegox.github.io/ElectronicColoringBook/



Electronic Codebook (ECB) mode encryption

Above: Encrypt with ECB

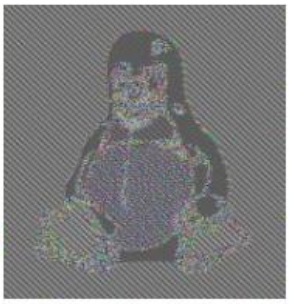


Electronic Codebook (ECB) mode decryption

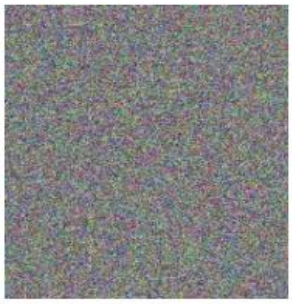
Above: Decrypt with ECB

ECB Disadvantages

Original image

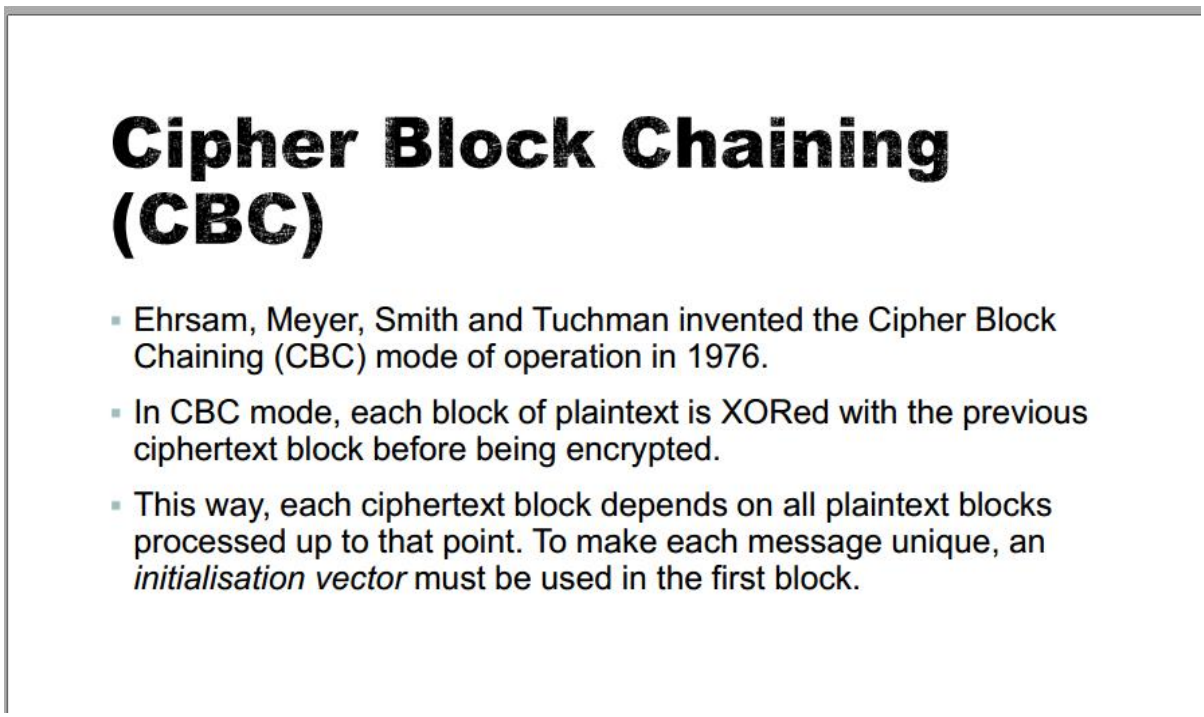


Encrypted using ECB mode



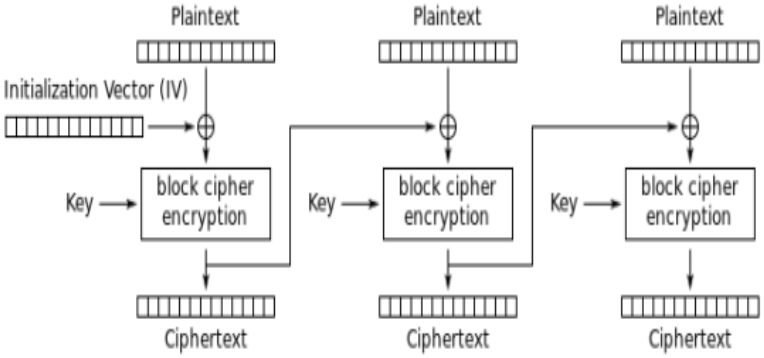
Modes other than ECB result in pseudo-randomness

- The image on the right is how the image might appear encrypted with CBC, CTR or any of the other more secure modes—indistinguishable from random noise
- ECB mode can also make protocols without integrity protection even more susceptible to replay attacks, since each block gets decrypted in

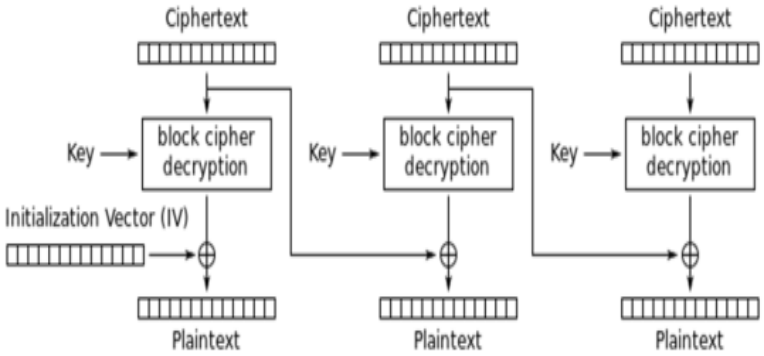


Cipher Block Chaining

Cipher Block Chaining (CBC)



Cipher Block Chaining (CBC) mode encryption



Cipher Block Chaining (CBC) mode decryption

Cipher Block Chaining (CBC)

- If the first block has index 1, the mathematical formula for CBC encryption is
$C_i = E_K(P_i \oplus C_{i-1}), C_0 = IV$
-
- while the mathematical formula for CBC decryption is
- $P_i = D_K(C_i) \oplus C_{i-1}, C_0 = IV.$
- CBC has been the most commonly used mode of operation. Its main drawbacks are that encryption is sequential (i.e., it cannot be parallelised), and that the message must be padded to a multiple of the cipher block size. One way to handle this last issue is through the method known as ciphertext stealing. Note that a one-bit change in a plaintext or IV affects all following ciphertext blocks.

Cipher Block Chaining (CBC)

- Decrypting with the incorrect IV causes the first block of plaintext to be corrupt but subsequent plaintext blocks will be correct.
- This is because a plaintext block can be recovered from two adjacent blocks of ciphertext. As a consequence, decryption can be parallelized.
  - Note that a one-bit change to the ciphertext causes complete corruption of the corresponding block of plaintext, and inverts the corresponding bit in the following block of plaintext, but the rest of the blocks remain intact. This peculiarity is exploited in different padding oracle attacks, such as POODLE.
- **Explicit Initialisation Vectors** takes advantage of this property by prepending a single random block to the plaintext. Encryption is done as normal, except the IV does not need to be communicated to the decryption routine. Whatever IV decryption uses, only the random block is "corrupted". It can be safely discarded and the rest of the decryption is the original plaintext.

Stream Cipher

- A stream cipher is a symmetric key cipher where plaintext digits are combined with a pseudorandom cipher digit stream (keystream).
- In a stream cipher each plaintext digit is encrypted one at a time with the corresponding digit of the keystream, to give a digit of the ciphertext stream.
- In practice, a digit is typically a bit and the combining operation an exclusive-or (XOR)
- Stream ciphers represent a different approach to symmetric encryption from block ciphers. Block ciphers operate on large blocks of digits with a fixed, unvarying transformation.

Stream Cipher

- Stream ciphers based on a proven unbreakable cipher, **the one-time pad (OTP),** sometimes known as the Vernam cipher.
- A one-time pad uses a keystream of completely random digits.
  - The keystream is combined with the plaintext digits one at a time to form the ciphertext. The keystream must be generated completely at random with at least the same length as the plaintext and cannot be used more than once. This makes the system very cumbersome to implement in practice, and as a result the one-time pad has not been widely used, except for the most critical applications.
- A stream cipher uses smaller and more convenient key such as 128 bits. Using the key to generate a pseudorandom keystream which can be combined with the plaintext digits in a similar fashion to the one-time pad. However, this comes at a cost. The keystream is now pseudorandom and so is not truly random. The proof of security associated with the one-time pad no longer holds. It is quite possible for a stream cipher to be completely unsecure