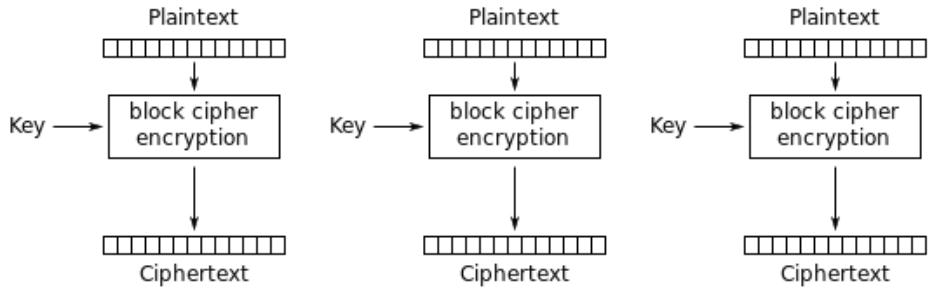
Assignment

Andreas Dedousis

AES ECB

- ECB = Electronic Code Book
- The simplest encryption mode
- The message is divided into blocks, and each block is encrypted separately
- Disadvantage
  - Identical plaintext blocks are encrypted into identical ciphertext blocks



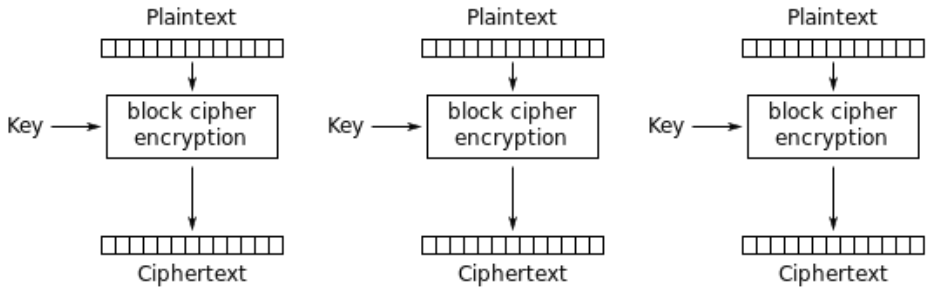
Electronic Codebook (ECB) mode encryption

Key Derivation Function (KDF)

- Key size: 128 or 256 bits
- Generated by random numbers
- Derived from passwords using hash functions and stretching
- EVP
  - Select a cipher (mode and key size)
  - Select a hash function
  - Use the above as arguments for the keygen function
  - Convert the password bytes to key

AES-ECB Encryption

- Plaintext is encrypted in blocks using the key
- Blocks have a fixed size
- The ciphertext may be larger than the plaintext due to padding on the last block
- The ciphertext is always aligned to the block size



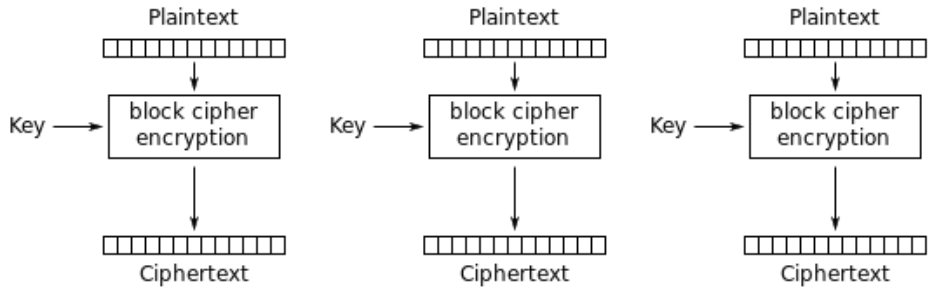
Electronic Codebook (ECB) mode encryption

AES-ECB Encryption

- Create a new encryption context
- Initialize it with the appropriate mode and key size
- Update the ciphertext
- Finalize the encryption
- Free the context

AES-ECB Decryption

- Ciphertext is decrypted in blocks using the key
- Blocks have a fixed size
- The plaintext may be smaller than the ciphertext due to padding on the last block
- The plaintext is not always aligned to the block size!



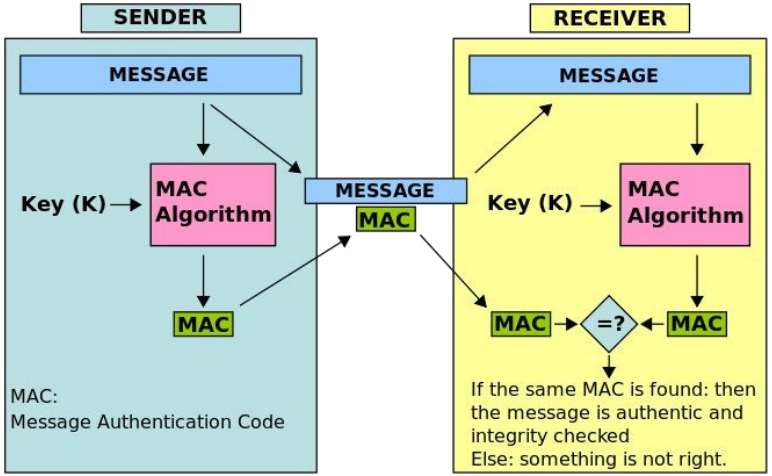
Electronic Codebook (ECB) mode encryption

AES-ECB Decryption

- Create a new decryption context
- Initialize it with the appropriate mode and key size
- Update the plaintext
- Finalize the decryption
- Free the context
- Remember to keep track of plaintext’s size!

Cipher-based Message Authentication Code (CMAC)

- The sender generates the CMAC using the message and the key
- The CMAC is appended to the message
- The receiver recalculates the message's CMAC and compares it to the one provided by the sender



CMAC Generation

- Create a new CMAC context
- Initialize it with the appropriate mode and key size
- Update the CMAC
- Finalize the CMAC
- Free the context

CMAC Verification

- The CMAC appended at the end of the message and has a fixed size
- Decrypt the message and save the CMAC
- Recalculate the CMAC as when generating it
- Compare the two CMACs