COMP 3704 Computer Security

Christian Grothoff
christian@grothoff.org

http://grothoff.org/christian/

Block Ciphers

- Provide encryption function E_K
- Operate on blocks of data (usually 64, 128 or 256 bits)
- Can be efficiently implemented in software (megabytes / second)

Requirements

- Hide patterns in input
- Error detection
- Error recovery
- Output size
- Allow re-use of cipher (with same key)
- Parallel execution

Electronic Codebook Mode

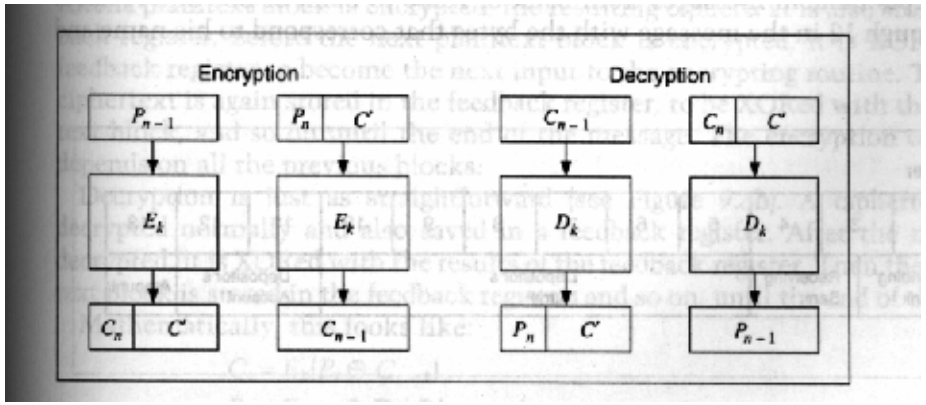
- A block of plaintext is encrypted into a block of ciphertext.
- The same block of plaintext always results in the same ciphertext.

$\Rightarrow$ For a given key, a (large) codebook can be constructed.

$\Rightarrow$ Parallel encryption and decryption are possible.

$\Rightarrow$ Facilitates certain attacks (repeated transmission, substitution, known-plaintext).

Ciphertext stealing in ECB mode



Cipher Block Chaining Mode

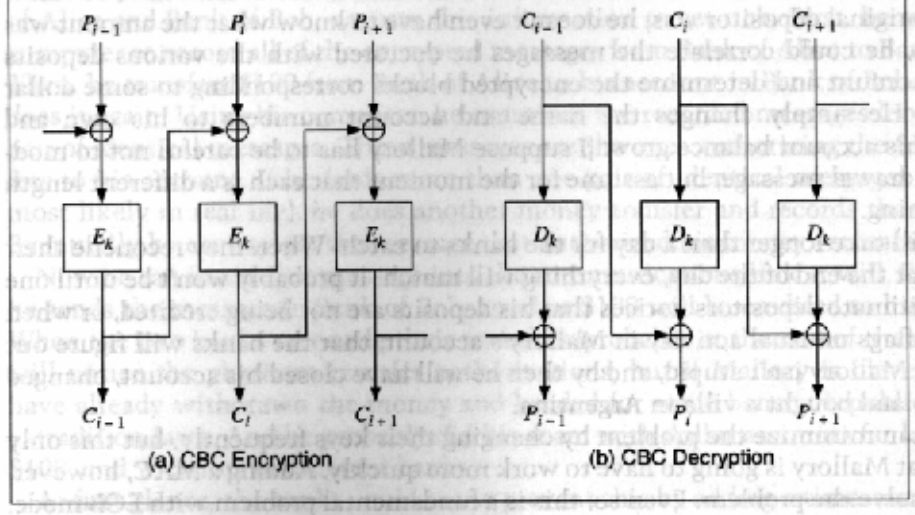
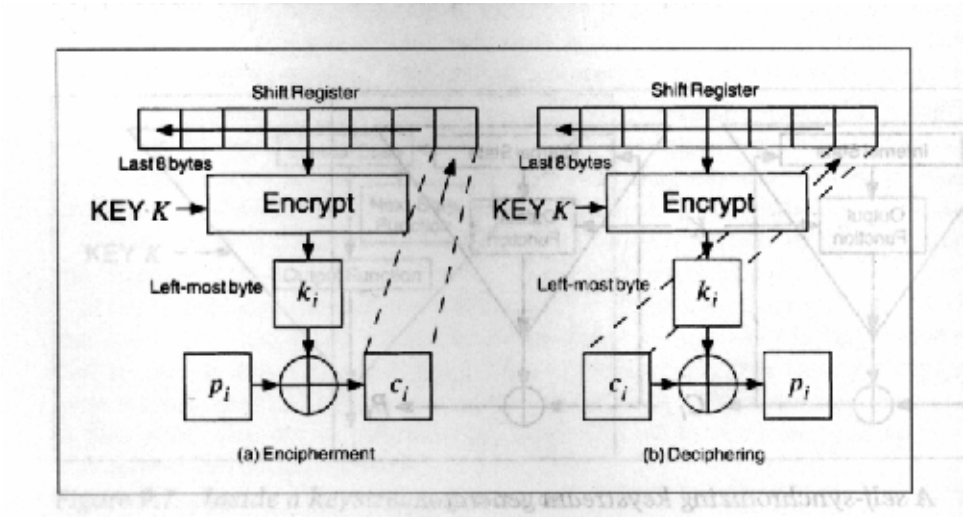


Figure 9.3 Cipher block chaining mode.

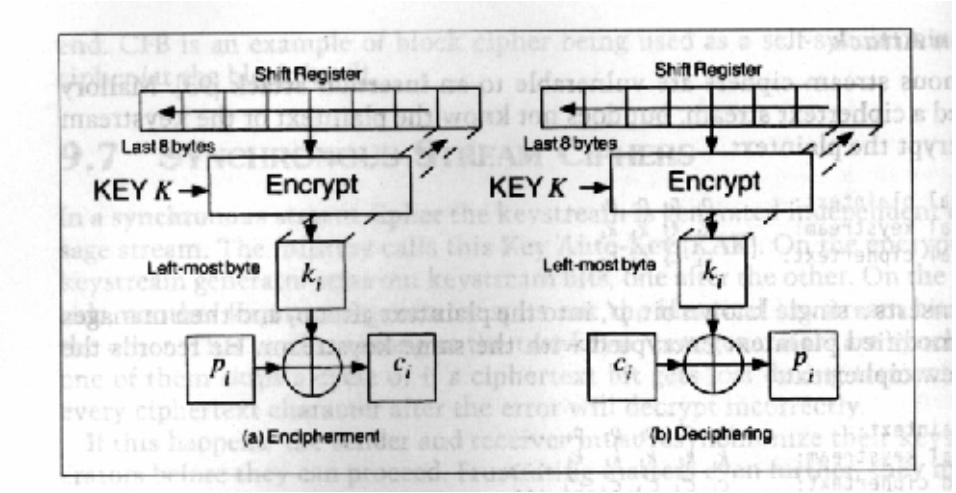
Stream Ciphers

- Generates a (random) stream of bits
- Plaintext is XOR'ed with the stream
- Stream generators are essentially glorified, keyed PRNGs

Cipher-Feedback Mode



Output-Feedback Mode



Choosing a Cipher Mode

- Default should be CBC.
- Consider CFB if single-character transmission is important (ssh, telnet).
- Consider OFB for systems with low-latency requirements for encryption (preprocessing!)
- ECB is only acceptable if replay is not a concern and random access / parallelization is crucial.

Also, pay attention to the format of the transmitted message (include length and CRC or MAC).

Choosing a Cipher Type

- Use block ciphers for software.
- Consider stream ciphers for streaming hardware.

Interleaving

- If parallel processing over n processors is desired,
- send n streams interleaved!

This does not enable out-of-order encryption (you need ECB mode for that).

Questions

?

Problem

Two banks transmit money transfer messages using ECB. Each message consists of two blocks. The first block contains a timestamp, the amount to transfer and the identity of the sending bank. The second block contains the identity of the receiving bank and the account number of the receiver.

How can Mallory get rich?