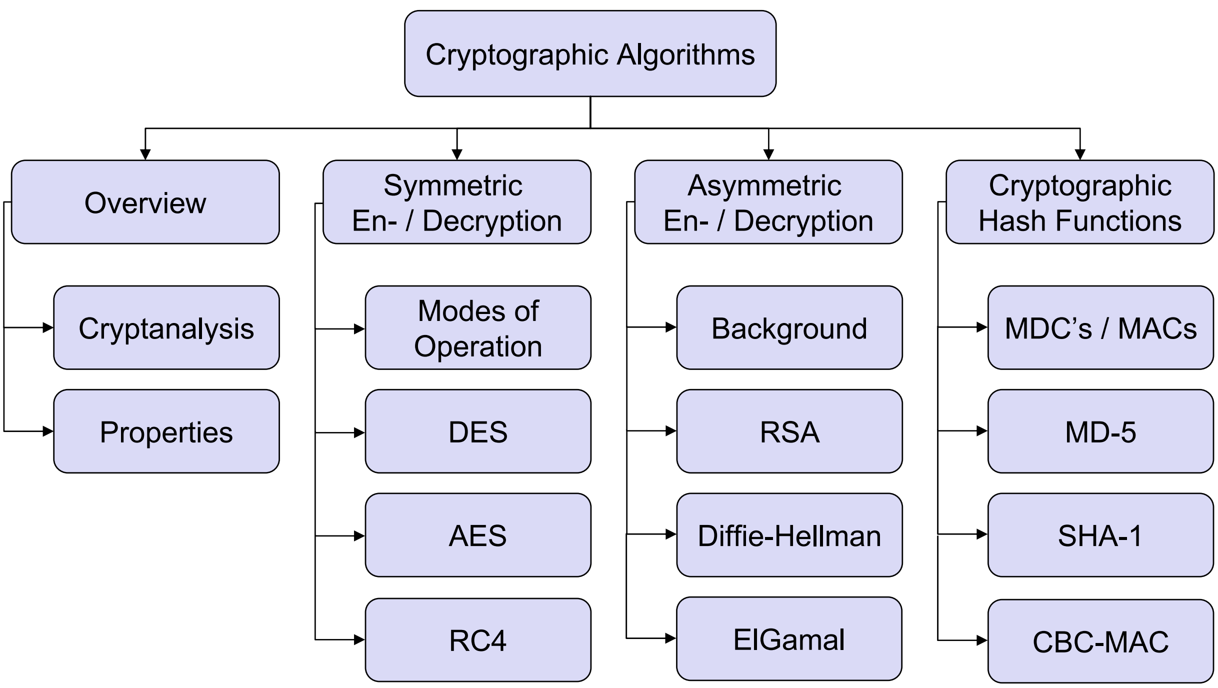
Chair for Network Architectures and Services
Department of Informatics
TU München – Prof. Carle

Network Security

Chapter 2 Basics
2.1 Symmetric Cryptography

- Overview of Cryptographic Algorithms
- Attacking Cryptographic Algorithms
- Historical Approaches
- Foundations of Modern Cryptography
- Modes of Encryption
- Data Encryption Standard (DES)
- Advanced Encryption Standard (AES)

Cryptographic algorithms: outline



Cryptographic algorithms: overview

- During this course two main applications of cryptographic algorithms are of principal interest:
  - *Encryption* of data: transforms plaintext data into ciphertext in order to conceal its meaning
  - *Signing* of data: computes a *check value* or *digital signature* of a given plain- or ciphertext, that can be verified by some or all entities who are able to access the signed data
- Some cryptographic algorithms can be used for both purposes, some are only secure and / or efficient for one of them.
- Principal categories of cryptographic algorithms:
  - *Symmetric cryptography* using 1 key for en-/decryption or signing/checking
  - *Asymmetric cryptography* using 2 different keys for en-/decryption or signing/checking
  - *Cryptographic hash functions* using 0 keys (the "key" is not a separate input but "appended" to or "mixed" with the data).

Attacking cryptography (1): Cryptanalysis

- *Cryptanalysis* is the process of attempting to discover the plaintext and / or the key
- Types of cryptanalysis:
  - *Ciphertext only:* work on ciphertext only; hope that specific patterns of the plaintext have remained in the ciphertext (frequencies of letters, digraphs, etc.)
  - *Known ciphertext / plaintext pairs*
  - *Chosen plaintext or chosen ciphertext*
  - Newer developments: *differential cryptanalysis, linear cryptanalysis*
- Cryptanalysis of public key cryptography:
  - The fact that one key is publicly exposed may be exploited
  - Public key cryptanalysis is more aimed at breaking the cryptosystem itself and is closer to pure mathematical research than to classic cryptanalysis
  - Important directions:
    - Computation of discrete logarithms
    - Factorization of large integers

Attacking cryptography (2): brute force attack

- The *brute force attack* tries every possible key until it finds an intelligible plaintext:
  - Every cryptographic algorithm can in theory be attacked by brute force
  - On average, half of all possible keys will have to be tried

Average Time Required for Exhaustive Key Search

Key Size [bit]	Number of keys	Time required at 1 encryption / µs	Time required at 10^6 encryption/µs
32	$2^{32} = 4.3 * 10^9$	2^{31} µs = 35.8 minutes	2.15 milliseconds
56	$2^{56} = 7.2 * 10^{16}$	2^{55} µs = 1142 years	10.01 hours
128	$2^{128} = 3.4 * 10^{38}$	2^{127} µs = $5.4 * 10^{24}$ years	$5.4 * 10^{18}$ years

- 1 encryption / µs: 100 Clock cycles of a 100 MHz processor
- 10^6 encryptions / µs: Clock cycles using 500 parallel 2GHz processors

Attacking cryptography (3): How large is large?

Reference Numbers Comparing Relative Magnitudes

Reference	Magnitude
Seconds in a year	$\approx 3 * 10^7$
Seconds since creation of solar system	$\approx 2 * 10^{17}$
Clock cycles per year (3 GHz computer)	$\approx 1 * 10^{17}$
Binary strings of length 64	$2^{64} \approx 1.8 * 10^{19}$
Binary strings of length 128	$2^{128} \approx 3.4 * 10^{38}$
Binary strings of length 256	$2^{256} \approx 1.2 * 10^{77}$
Number of 75-digit prime numbers	$\approx 5.2 * 10^{72}$
Electrons in the universe	$\approx 8.37 * 10^{77}$

Classification of modern encryption algorithms

- The type of operations used for transforming plaintext to ciphertext:
  - *Substitution*, which maps each element in the plaintext (bit, letter, group of bits or letters) to another element
  - *Transposition,* which re-arranges elements in the plaintext
- The number of keys used:
  - *Symmetric ciphers,* which use the same key for en- / decryption
  - *Asymmetric ciphers,* which use different keys for en- / decryption
- The way in which the plaintext is processed:
  - *Stream ciphers* work on bit streams and encrypt one bit after another
  - *Block ciphers* work on blocks of width *b* with *b* depending on the specific algorithm.

Basic Kryptographic Principles

- Substitution
  - Individual characters are exchanged by other characters

  Types of substitution
  - simple substitution: operates on single letters
  - polygraphic substitution: operates on larger groups of letters
  - monoalphabetic substitution: uses fixed substitution over the entire message
  - polyalphabetic substitution: uses different substitutions at different sections of a message
- Transposition
  - The position of individual characters changes (Permutation)

Transposition: scytale

- Known as early as 7th century BC
- Principle:
  - Wrap parchment strip over a wooden rod of a fixed diameter and write letters along the rod.
  - Unwrap a strip and "transmit"
  - To decrypt, wrap a received over a wooden rod of the same diameter and read off the text.

- Example:

```
troops
headii
nthewe
stneed
moresu
pplies
```

⇨ `thnsm predd opoah nrlod eeeis iedus`

- Weakness:
  - Easy to break by finding a suitable matrix transposition.

Monoalphabetic substitution: Atbash

Jeremiah 25:25

And all the kings of the north, far and near, one with another, and all the kingdoms of the world, which are upon the face of the earth: and the king of Sheshach shall drink after them.

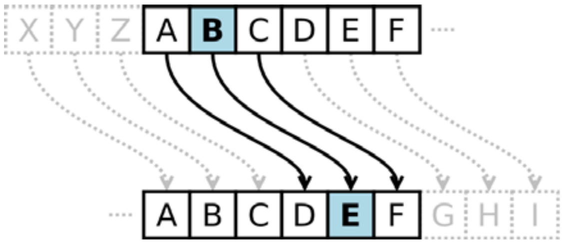
Atbash code: reversed Hebrew alphabet.

A Aleph א	B Beth ב	G Gimel ג	D Daleth ד	H He ה	WVFY Waw ו	Z Zajin ז	H Chet ח	T Tet ט	IJ Jod י	K Kaph כ ך	L Lamed ל	M Mem מ ם	N Nun נ ן	X Samech ס	O Ajin ע	P Pe פ ף	Z Sade צ ץ	Q Koph ק	R Resch ר	S Sin ש	T Taw ת
T Taw ת	S Sin ש	R Resch ר	Q Koph ק	Z Sade צ ץ	P Pe פ ף	O Ajin ע	X Samech ס	N Nun נ ן	M Mem מ ם	L Lamed ל	K Kaph כ ך	IJ Jod י	T Tet ט	H Chet ח	Z Zajin ז	WVFY Waw ו	H He ה	D Daleth ד	G Gimel ג	B Beth ב	A Aleph א

Sheshach ⇨ כ ך ש ש ⇨ ל ב ב ⇨ Babel

Monoalphabetic substitution: Caesar cipher

- Caesar code: left shift of alphabet by 3 positions.



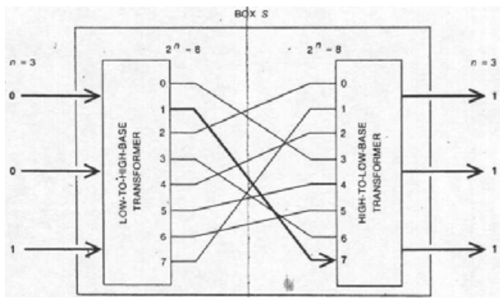
- Example (letter of Cicero to Caesar):
  `MDEHV RSNQNRQNV PHDH XHVXNPRQNZP`
  `HABES OPINIONIS MEAE TESTIMONIUM`

- Weakness: a limited number of possible substitutions. Easy to break by brute force!

Modern cryptography: S and P-boxes

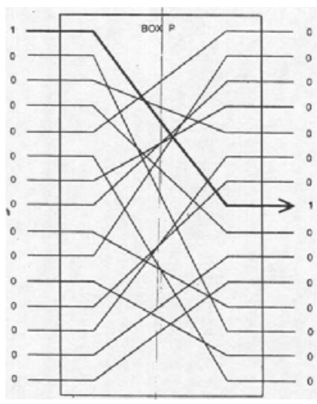
S-box:

- Block-wise **substitution** of binary digits.
- Resistant to attacks for sufficiently large block size; e.g. for n=128 it provides 2^{128} possible mappings.



P-box:

- Block-wise **permutation** of binary digits.
- Realizes a simple **transposition** cipher with maximal entropy.
- Problem: straightforward attacks exist.

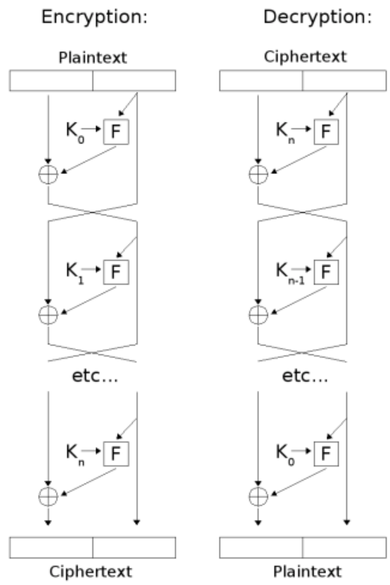


Feistel network: a product cipher of S and P-boxes

- A revival of the idea of a product cipher.
  - A product cipher is a combination of simple ciphers (e.g. S-box and P-box) to make the cipher more secure.
  - Rounds: This combination may be applied multiple times.
- Multiple rounds provide a cryptographically strong polyalphabetic substitution.
- Combination of substitution with transposition provides protection against specific attacks (frequency analysis).
- Follows the theoretical principles outlined by C. Shannon in 1949: combines “confusion” with “diffusion” to attain maximal entropy of a cipher text.
  - Confusion: cipher text statistics depend in a very complex way on plaintext statistics (approach: substitution in different rounds)
  - Diffusion: each digit in plaintext and in key influence many digits of cipher text (approach: many rounds with transposition)

A practical Feistel cipher

- A multiple-round scheme with separate keys per round.
- Goal: Encrypt plaintext block $P = L_0 \mid R_0$
- Function $f(K_i, R_{i-1})$ is algorithm-specific, usually a combination of permutations and substitutions.
- Invertible via a reverse order of rounds.
- 3 rounds suffice to achieve a pseudorandom permutation.
- 4 rounds suffice to achieve a strong pseudorandom permutation (i.e. it remains pseudorandom to an attacker with an oracle access to its inverse permutation).
- A foundation for a large number of modern symmetric ciphers: DES, Lucifer, Blowfish, RC5, Twofish, etc.



Feistel Cipher

Important properties of encryption algorithms

Consider, a sender is encrypting plaintext messages P_1, P_2, ... to ciphertext messages C_1, C_2, ...

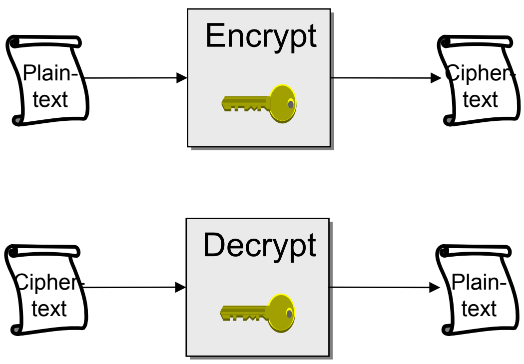
Then the following properties of the encryption algorithm are of special interest:

- *Error propagation* characterizes the effects of bit-errors during transmission of ciphertext on reconstructed plaintext $P_1´$, $P_2´$, ...
  - Depending on the encryption algorithm there may be one or more erroneous bits in the reconstructed plaintext per erroneous ciphertext bit

- *Synchronization* characterizes the effects of lost ciphertext data units on the reconstructed plaintext
  - Some encryption algorithms cannot recover from lost ciphertext and need therefore explicit re-synchronization in case of lost messages
  - Other algorithms do automatically re-synchronize after 0 to n (n depending on the algorithm) ciphertext bits

Symmetric Encryption

- General description:
  - The same key $K_{A,B}$ is used for enciphering and deciphering of messages:



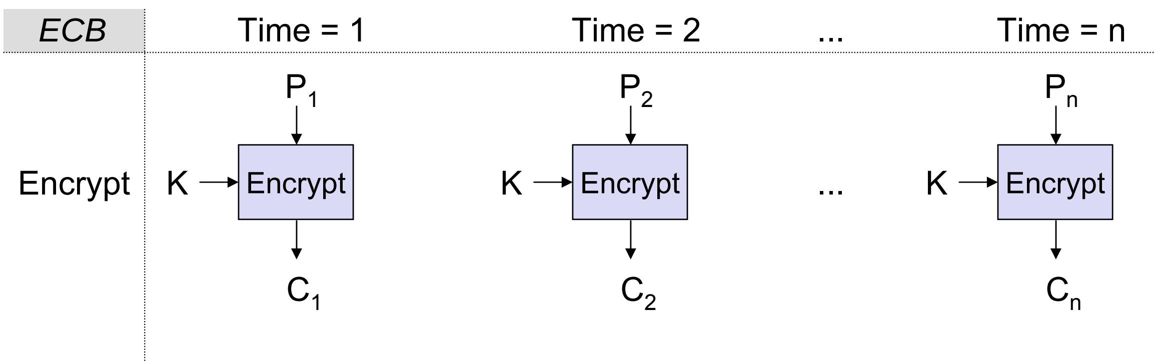
- Notation
  - If P denotes the plaintext message, $E(K_{A,B}, P)$ denotes the cipher text. The following holds: $D(K_{A,B}, E(K_{A,B}, P)) = P$
  - Alternatively we sometimes write $\{P\}_{K_{A,B}}$ or $E_{K_{A,B}}(P)$ for $E(K_{A,B}, P)$
- Symmetric encryption
  - $E_{K_{A,B}}$ is at least an injective, often a bijective function
  - $D_{K_{A,B}}$ is the inverse function of $E_{K_{A,B}}$: $D_{K_{A,B}} = (E_{K_{A,B}})^{-1}$
- Examples: DES, 3DES, AES, Twofish, RC4

Modes of Encryption

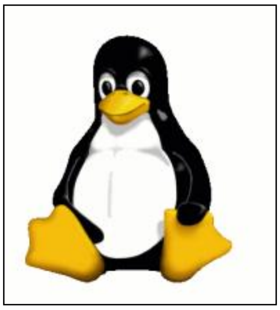
- Block ciphers operate on 128-256 bits. How can one encrypt longer messages? Answer:
  - A plaintext *p* is segmented in blocks p_1, p_2, ... each of length *b* or of length $j<b$ when payload length is smaller or not a multiple of *b*. *b* denotes the block size of the encryption algorithm.
  - The ciphertext *c* is the combination of c_1, c_2, ... where c_i denotes the result of the encryption of the i^{th} block of the plaintext message
  - The entities encrypting and decrypting a message have agreed upon a key *K*.
- Modes where the plaintext is input to the block cipher. Examples:
    - Electronic Code Book Mode (ECB), Cipher Block Chaining Mode (CBC)
- Modes where the plaintext is XORed with the output of a block cipher
  - A pseudorandom stream of bits, called *key stream* is generated from the symmetric key *K* and a specific input per block,
    e.g. E(K,“Block 1”), E(K,”Block 2”), E(K,”Block 3”), …
  - Examples
    - Output Feedback Mode (OFB), Counter Mode (CTR)

Symmetric Block Ciphers - Modes of Encryption – ECB (1)

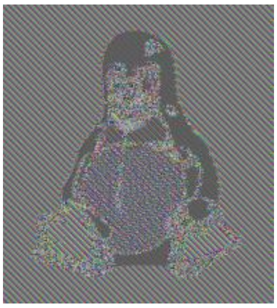
- *Electronic Code Book Mode (ECB):*
  - Every block p_i of length *b* is encrypted independently: $c_i = E(K, p_i)$
  - A bit error in one ciphertext block c_i results in a completely wrongly recovered plaintext block p_i' (subsequent blocks are not affected)
  - Loss of synchronization does not have any effect if integer multiples of the block size *b* are lost.
    If any other number of bits are lost, explicit re-synchronization is needed.
  - Drawback: identical plaintext blocks are encrypted to identical ciphertext!



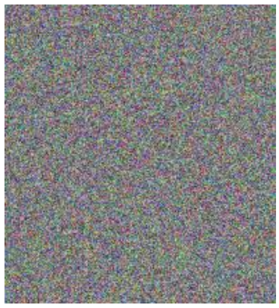
Symmetric Block Ciphers - Modes of Encryption – ECB (2)



Original



Encrypted using ECB mode



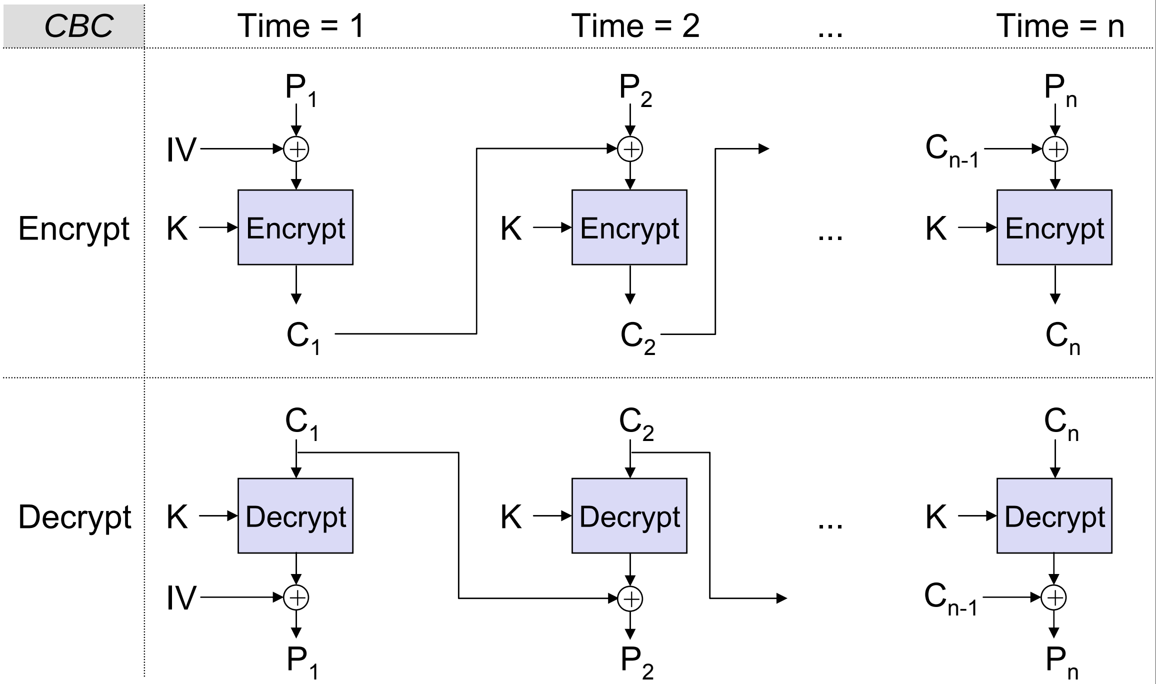
Encrypted using other modes

Source: http://www.wikipedia.org/

Symmetric Block Ciphers - Modes of Encryption – CBC (1)

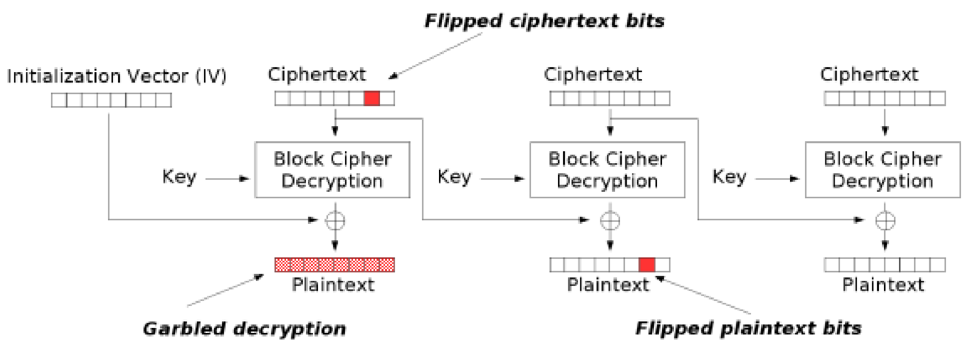
- *Cipher Block Chaining Mode (CBC):*
  - Before encrypting a plaintext block p_i , it is XORed (⊕) with the preceding ciphertext block c_{i-1}:
    - $c_i = E(K, c_{i-1} \oplus p_i)$
    - $p_i' = c_{i-1} \oplus D(K, c_i)$
  - Both parties agree on an *initial value* for c_i *called Initialization Vector (IV)*
    - c_0 = IV
- Properties:
  - Advantage: identical plaintext blocks are encrypted to non-identical ciphertext.
  - Error propagation:
    - A distorted ciphertext block results in two distorted plaintext blocks, as p_i' is computed using c_{i-1} and c_i
  - Synchronisation:
    - If the number of lost bits is a multiple integer of *b*, one additional block p_{i+1} is misrepresented before synchronization is re-established.
      If any other number of bits are lost explicit re-synchronization is needed.
  - Applicable for
    - Encryption
    - Integrity check: use last block of CBC as Message Authentication Code (MAC)

Symmetric Block Ciphers - Modes of Encryption – CBC (2)



CBC Error Propagation

- A distorted ciphertext block results in two distorted plaintext blocks, as $p_i´$ is computed using c_{i-1} and c_i



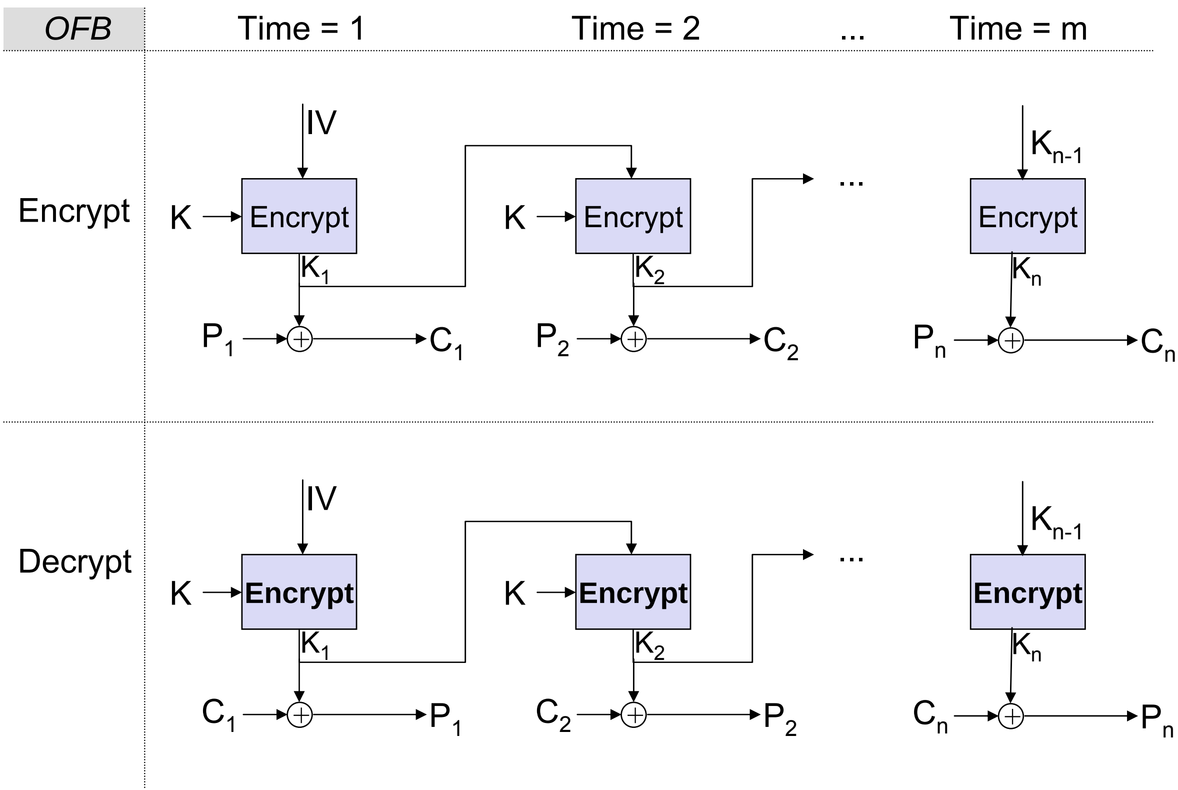
Modification attack or transmission error for CBC

Source: http://www.wikipedia.org/

Symmetric Block Ciphers - Modes of Encryption – OFB (1)

- *Output Feedback Mode (OFB):*
  - The block encryption algorithm is used to generate a key stream that depends only on *K* and *IV*
    - $K_0 = IV$
    - $K_i = E(K, K_{i-1})$
    - $C_i = P_i \oplus K_i$
  - The plaintext blocks are XORed with the pseudo-random sequence to obtain the ciphertext and vice versa

Symmetric Block Ciphers - Modes of Encryption – OFB (2)



Symmetric Block Ciphers - Modes of Encryption – OFB (3)

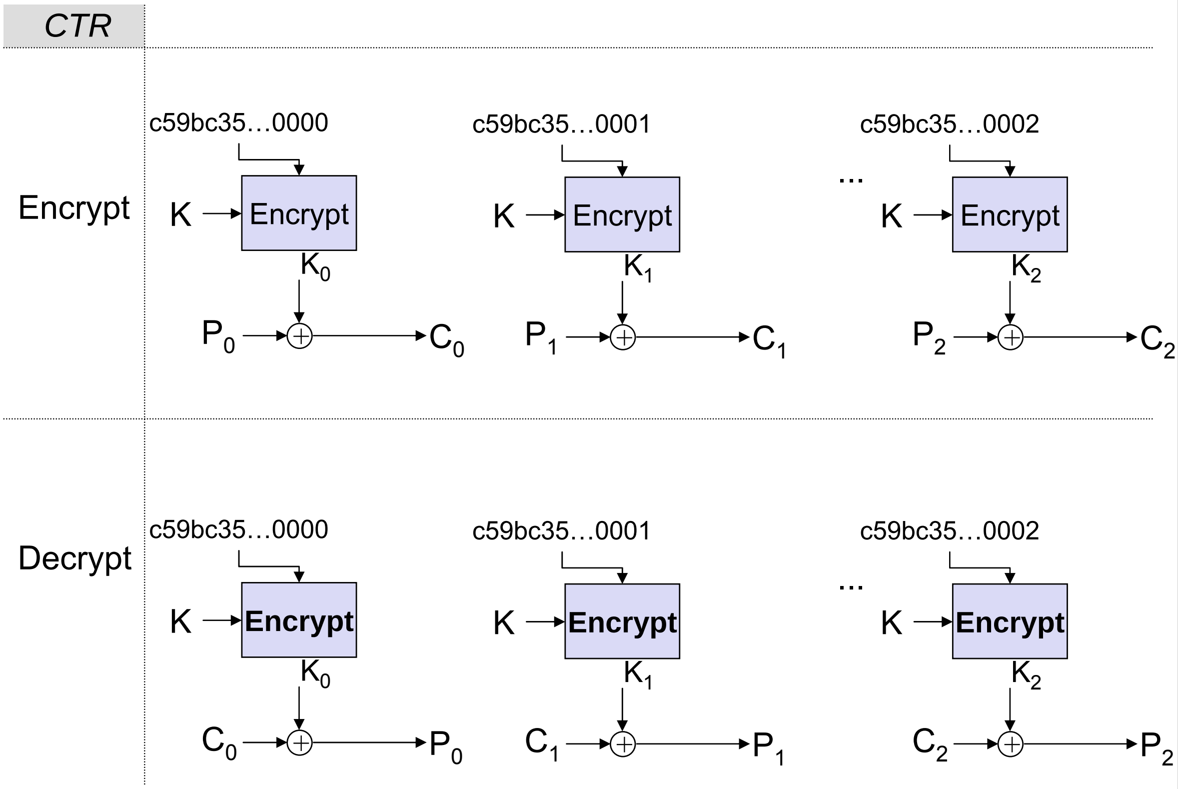
- Properties of OFB:
  - Error propagation:
    - Single bit errors result only in single bit errors ⇒ no error multiplication
  - Synchronisation:
    - If some bits are lost explicit re-synchronization is needed
  - Advantage:
    - The pseudo-random sequence can be pre-computed in order to keep the impact of encryption to the end-to-end delay low
  - Drawbacks:
    - It is possible for an attacker to manipulate specific bits of the plaintext

    → However, additional cryptographic means are can be used for message integrity

Symmetric Block Ciphers – Modes of Encryption - CTR (1)

- *Counter Mode (CTR)*
  - The block encryption algorithm is used to generate a key stream that depends on *K* and a counter function ctr_i .
  - The counter function can be simply an increment modulo 2^w, where *w* is a convenient register width, e.g.
    - $ctr_i = Nonce \mid\mid i$
  - The counter function does not provide any security other than the uniqueness of the input to the block cipher function *E*
  - The plaintext blocks are XORed with the pseudo-random sequence to obtain the ciphertext and vice versa
  - Putting everything together:
    - $K_i = E(K, Nonce \mid\mid i)$
    - $C_i = P_i \oplus K_i$

Symmetric Block Ciphers – Modes of Encryption - CTR (2)



Symmetric Block Ciphers – Modes of Encryption - CTR (3)

- Properties of CTR:
  - Error propagation:
    - Single bit errors result only in single bit errors $\Rightarrow$ no error multiplication
  - Synchronisation:
    - If some bits are lost explicit re-synchronization is needed.
  - Advantage:
    - The key stream can be pre-computed in order to keep the impact of encryption to the end-to-end delay low.
    - The computation of the key stream can be parallelized.
  - Drawbacks:
    - It is possible for an attacker to manipulate specific bits of the plaintext

    → However, additional cryptographic means are required for message integrity