Cryptographie M1

Lecture 1

Ludovic Perret
(slides from C. Bouillaguet and Damien Vergnaud)

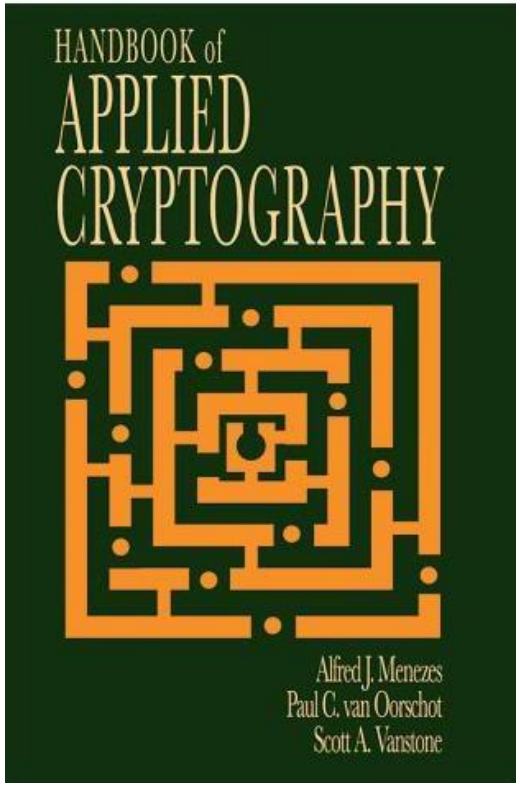
Sorbonne Université

2023 – 2024

References

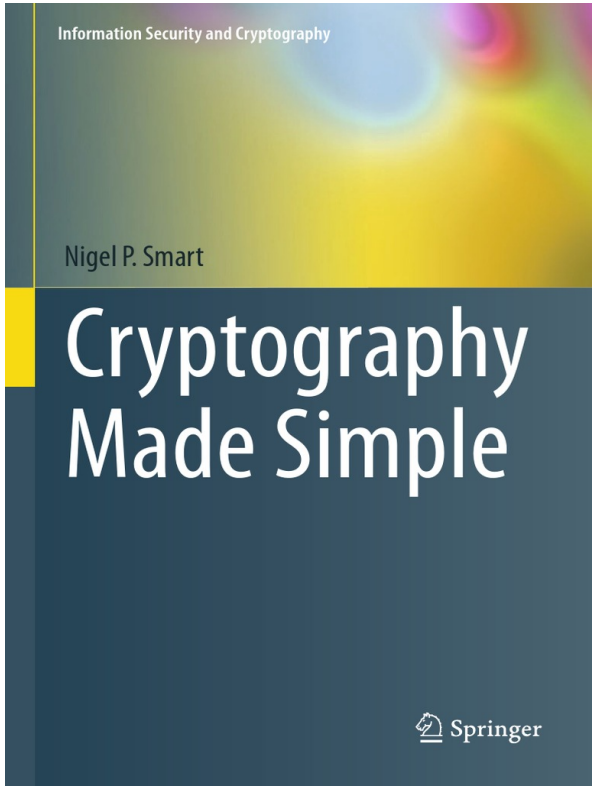
Cryptographie : Théorie et pratique
Douglas Stinson

References



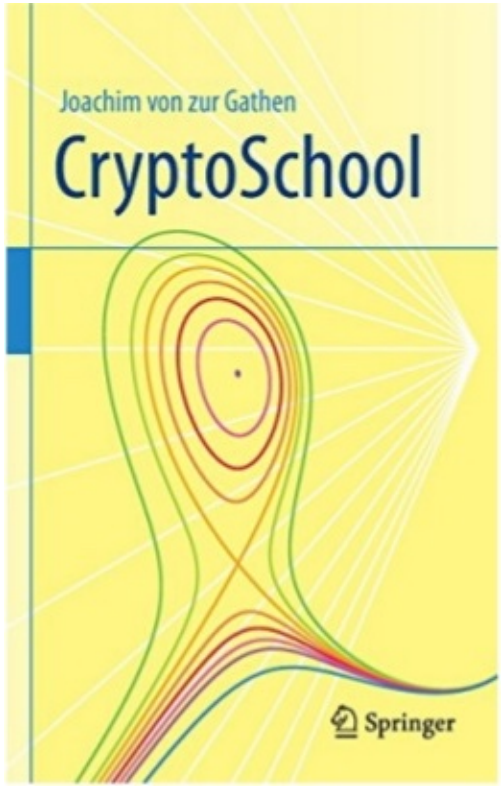
Handbook of Applied Cryptography
Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone

References



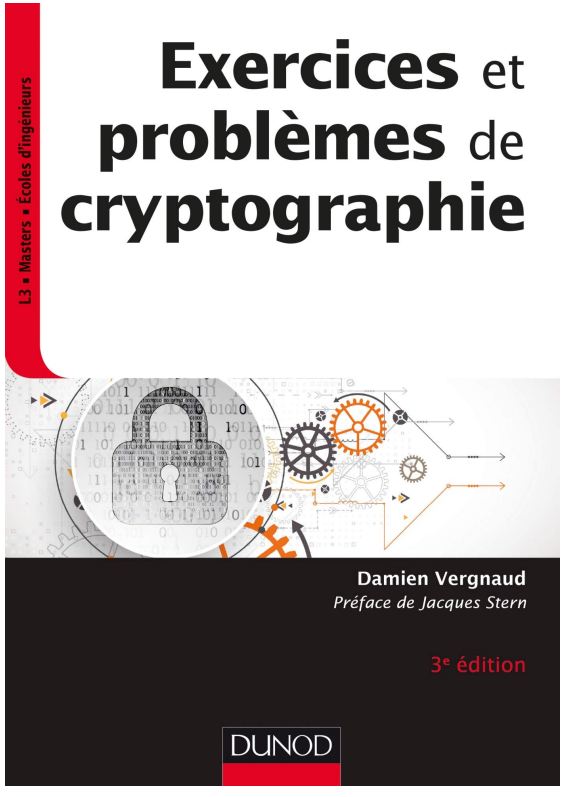
Cryptography Made Simple
Nigel P. Smart

References



CryptoSchool
Joachim von zur Gathen

References



Exercices et problèmes de cryptographie
Damien Vergnaud (Sorbonne Université, responsable ISEC)

Contents

Characters

Anissa

Characters

Billel

The basic goal: communication

internet, phone line, ...

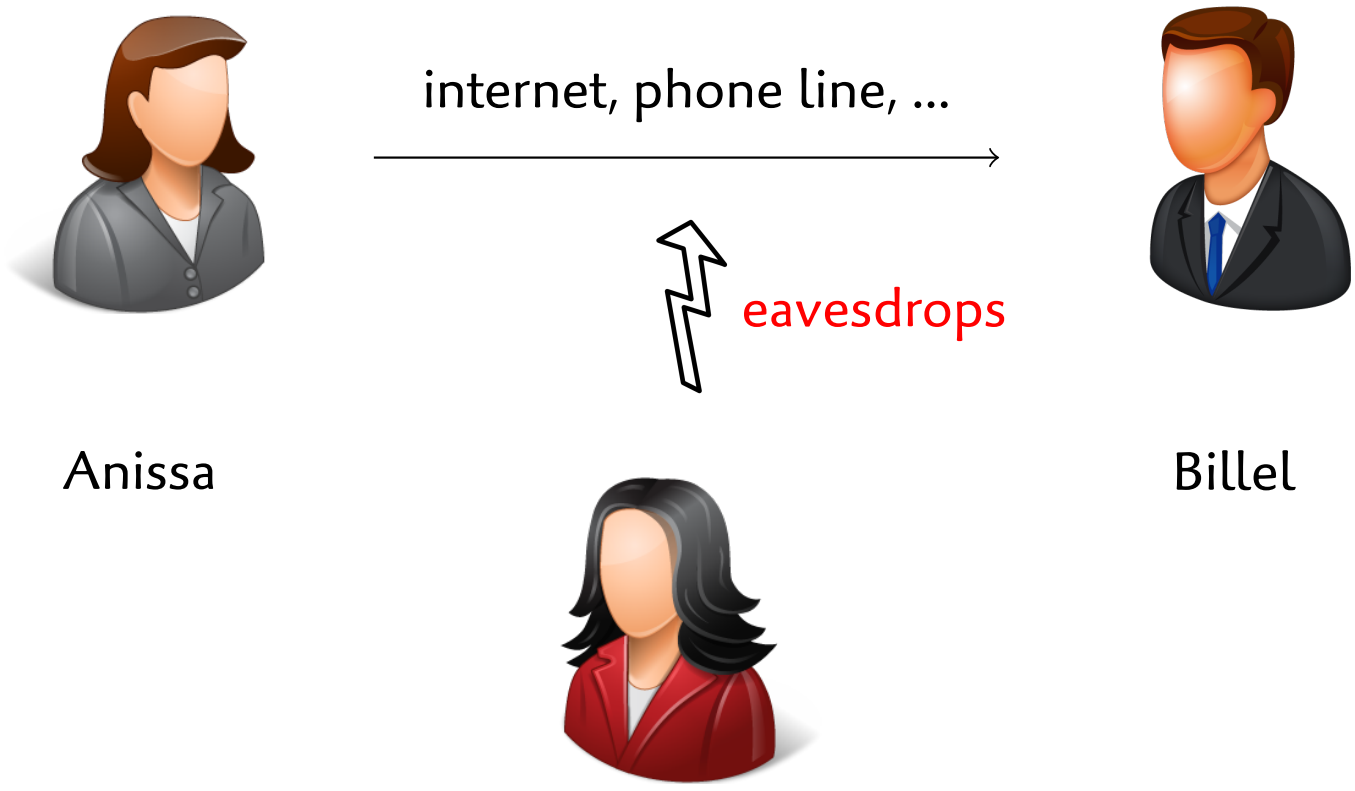
Anissa

Billel

Another character

Eve

The basic goal: **secure** communication



Information security objectives

Cryptology = practice and study of hiding information

confidentiality	keeping information secret from all but those who are authorized to see it
integrity	ensuring information has not been altered by unauthorized or unknown means
message authentication	corroborating the source of information
signature	a means to bind information to an entity
receipt	acknowledgement that information has been received
anonymity	concealing the identity of an entity involved in some process
non-repudiation	preventing the denial of previous commitments or actions
etc	*etc*

Information security objectives

Cryptology = practice and study of hiding information

confidentiality	keeping information secret from all but those who are authorized to see it
integrity	ensuring information has not been altered by unauthorized or unknown means
message authentication	corroborating the source of information
signature	a means to bind information to an entity
receipt	acknowledgement that information has been received
anonymity	concealing the identity of an entity involved in some process
non-repudiation	preventing the denial of previous commitments or actions
etc	*etc*

Information security objectives

Cryptology = practice and study of hiding information

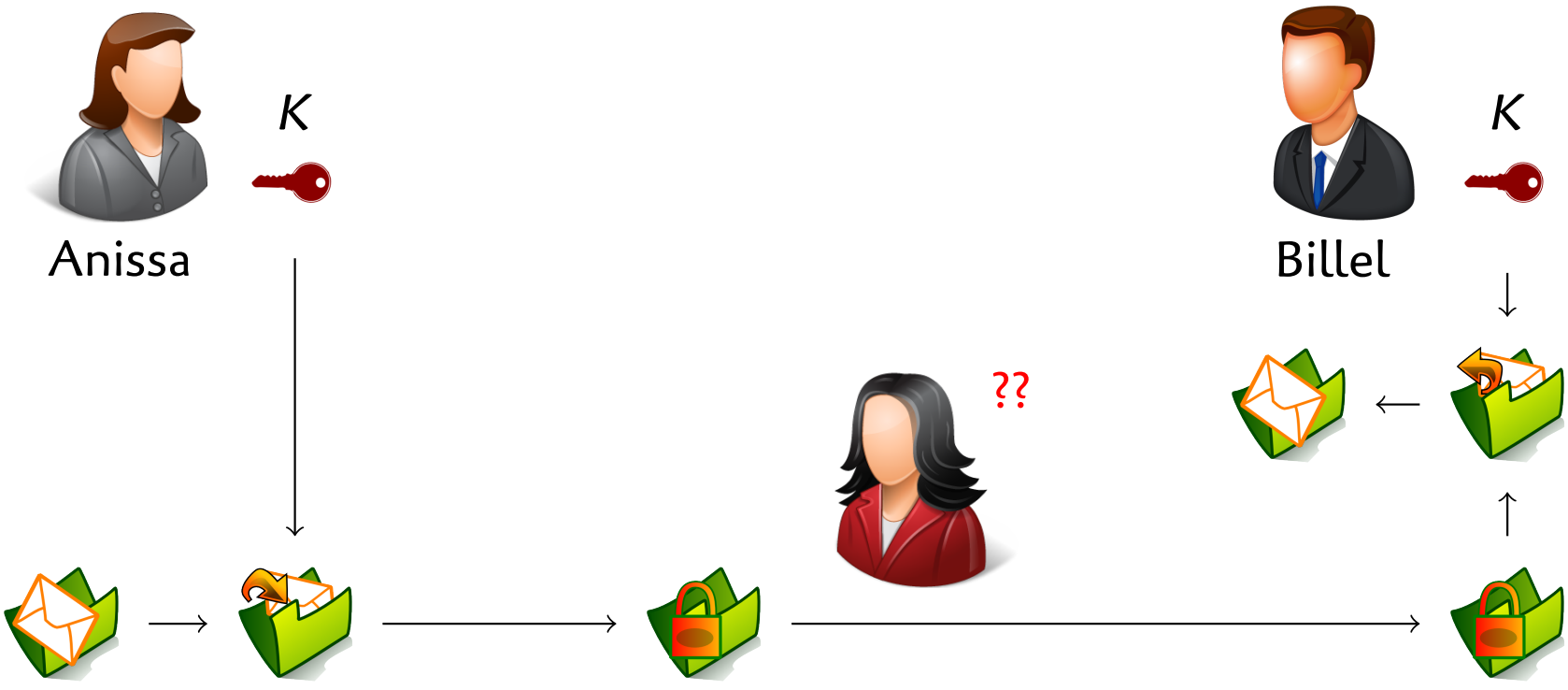
confidentiality	keeping information secret from all but those who are authorized to see it
integrity	ensuring information has not been altered by unauthorized or unknown means
message authentication	corroborating the source of information
signature	a means to bind information to an entity
receipt	acknowledgement that information has been received
anonymity	concealing the identity of an entity involved in some process
non-repudiation	preventing the denial of previous commitments or actions
etc	*etc*

Terminology

- Cryptography
- Crytanalysis (Cryptanalyst)
- Cryptology
- Cipher/Encryption Algorithm
- Encryption/Encipherment
- Decryption/Decipherment
- Plaintext
- Ciphertext

Secret Key Cryptosystems

Symmetric encryption: Anissa and Billel share a "key" K



- Billel can use the same method to send messages to Anissa.
  $\rightsquigarrow$ **symmetric setting**
- How did Anissa and Billel establish K?

Kerckhoffs's principle

In 1883 Auguste Kerckhoffs wrote two journal articles on *La Cryptographie Militaire*:

- Le système doit être matériellement, sinon mathématiquement, indéchiffrable
  - **The system must be practically, if not mathematically, indecipherable**
- Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi
  - **It must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience**
- La clef doit pouvoir en être communiquée et retenue sans le secours de notes écrites, et être changée ou modifiée au gré des correspondants
  - **Its key must be communicable and retainable without the help of written notes, and changeable or modifiable at the will of the correspondents**

Kerckhoffs's principle

In 1883 Auguste Kerckhoffs wrote two journal articles on *La Cryptographie Militaire*:

- Le système doit être matériellement, sinon mathématiquement, indéchiffrable
  - **The system must be practically, if not mathematically, indecipherable**
- Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi
  - **It must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience**
- La clef doit pouvoir en être communiquée et retenue sans le secours de notes écrites, et être changée ou modifiée au gré des correspondants
  - **Its key must be communicable and retainable without the help of written notes, and changeable or modifiable at the will of the correspondents**

Kerckhoffs's principle

In 1883 Auguste Kerckhoffs wrote two journal articles on *La Cryptographie Militaire*:

- Le système doit être matériellement, sinon mathématiquement, indéchiffrable
  - **The system must be practically, if not mathematically, indecipherable**
- Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi
  - **It must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience**
- La clef doit pouvoir en être communiquée et retenue sans le secours de notes écrites, et être changée ou modifiée au gré des correspondants
  - **Its key must be communicable and retainable without the help of written notes, and changeable or modifiable at the will of the correspondents**

Kerckhoffs's principle

- Il faut qu'il soit applicable à la correspondance télégraphique
  - **It must be applicable to telegraphic correspondence**
- Il faut qu'il soit portatif, et que son maniement ou son fonctionnement n'exige pas le concours de plusieurs personnes
  - **It must be portable, and its usage and function must not require the concourse of several people**
- Enfin, il est nécessaire, vu les circonstances qui en commandent l'application, que le système soit d'un usage facile, ne demandant ni tension d'esprit, ni la connaissance d'une longue série de règles à observer
  - **Finally, it is necessary, given the circumstances that command its application, that the system be easy to use, requiring neither mental strain nor the knowledge of a long series of rules to observe**

Kerckhoffs's principle

- Il faut qu'il soit applicable à la correspondance télégraphique
  - **It must be applicable to telegraphic correspondence**
- Il faut qu'il soit portatif, et que son maniement ou son fonctionnement n'exige pas le concours de plusieurs personnes
  - **It must be portable, and its usage and function must not require the concourse of several people**
- Enfin, il est nécessaire, vu les circonstances qui en commandent l'application, que le système soit d'un usage facile, ne demandant ni tension d'esprit, ni la connaissance d'une longue série de règles à observer
  - **Finally, it is necessary, given the circumstances that command its application, that the system be easy to use, requiring neither mental strain nor the knowledge of a long series of rules to observe**

Kerckhoffs's principle

- Il faut qu'il soit applicable à la correspondance télégraphique
  - **It must be applicable to telegraphic correspondence**
- Il faut qu'il soit portatif, et que son maniement ou son fonctionnement n'exige pas le concours de plusieurs personnes
  - **It must be portable, and its usage and function must not require the concourse of several people**
- Enfin, il est nécessaire, vu les circonstances qui en commandent l'application, que le système soit d'un usage facile, ne demandant ni tension d'esprit, ni la connaissance d'une longue série de règles à observer
  - **Finally, it is necessary, given the circumstances that command its application, that the system be easy to use, requiring neither mental strain nor the knowledge of a long series of rules to observe**

Encryption: Security Notions

Encryption is supposed to provide confidentiality of the data.

But what exactly does this mean?

Security goal	But ...
Recovery of secret key is infeasible	True if data is sent in the clear
Obtaining plaintext from ciphertext is infeasible	Might be able to obtain half the plaintext
etc	*etc*

So what is a **secure** encryption scheme ?

Not an easy question to answer ...

Attackers should not be able to compute any information about m.

Encryption: Security Notions

Encryption is supposed to provide confidentiality of the data.

But what exactly does this mean?

Security goal	But ...
Recovery of secret key is infeasible	True if data is sent in the clear
Obtaining plaintext from ciphertext is infeasible	Might be able to obtain half the plaintext
etc	*etc*

So what is a **secure** encryption scheme ?

Not an easy question to answer ...

Attackers should not be able to compute any information about m.

How to formalize it ?

Attackers should not be able to compute any information about m.

Probabilistic approach

- M some random variable that takes values from $\mathcal{M}$
- K random variable distributed uniformly over $\mathcal{K}$
- $C = \mathcal{E}_K(M)$

Definition

An encryption scheme is perfectly secret if for every random variable M, every $m \in \mathcal{M}$ and every $c \in \mathcal{C}$ with $\Pr(C = c) > 0$:

$$\Pr(M = m) = \Pr(M = m | C = c)$$

$\rightsquigarrow$ C and M are independent

A perfectly secure scheme: **one-time pad**

Description

- $\ell \in \mathbb{N}$ a parameter. $\mathcal{M} = \mathcal{K} = \{0,1\}^\ell$.
- Let $\oplus$ denote component-wise XOR.
- **Vernam's cipher:** $\mathsf{Enc}(K, m) = m \oplus K$ and $\mathsf{Dec}(K, c) = c \oplus K$.

- One-time pad is perfectly secret!

$$\begin{aligned} \Pr(C = c | M = m) &= \Pr(K \oplus M = c | M = m) \\ &= \Pr(K = m \oplus c | M = m) = 2^{-\ell} \end{aligned}$$

- Each key cannot be used more than once!

$$\mathsf{Enc}(K, m_0) \oplus \mathsf{Enc}(K, m_1) = (m_0 \oplus K) \oplus (m_1 \oplus K) = m_0 \oplus m_1$$

- One time-pad is optimal in the class of perfectly secret schemes

Does encryption guarantee message integrity?

- **Idea:**
  - Anissa encrypts m and sends $c = \mathrm{Enc}(K, m)$ to Billel.
  - Billel computes $\mathrm{Dec}(K, m)$, and if it "makes sense" accepts it.
- **Intuition:** only Anissa knows K, so nobody else can produce a valid ciphertext.

It does not work!

Example

one-time pad.

Need a way to ensure that data arrives at destination in its original form (as sent by the sender and it is coming from an authenticated source)

Does encryption guarantee message integrity?

- **Idea:**
  - Anissa encrypts m and sends $c = \mathrm{Enc}(K, m)$ to Billel.
  - Billel computes $\mathrm{Dec}(K, m)$, and if it "makes sense" accepts it.
- **Intuition:** only Anissa knows K, so nobody else can produce a valid ciphertext.

It does not work!

Example

one-time pad.

Need a way to ensure that data arrives at destination in its original form (as sent by the sender and it is coming from an authenticated source)

Outline

Block ciphers

- Block cipher
  - deterministic algorithm
  - operates on fixed-length groups of bits, called **blocks**,
  - an unvarying transformation specified by a **symmetric key**.
- Design of block ciphers
  - based on the concept of an **iterated product cipher**
  - suggested and analyzed by Claude Shannon
  - by combining simple operations such as substitutions and permutations
- Two main techniques
  - **Feistel network** or Feistel scheme
  - **substitution-permutation networks** (SPN network)

Block ciphers

- Block cipher
  - deterministic algorithm
  - operates on fixed-length groups of bits, called **blocks**,
  - an unvarying transformation specified by a **symmetric key**.
- Design of block ciphers
  - based on the concept of an **iterated product cipher**
  - suggested and analyzed by Claude Shannon
  - by combining simple operations such as substitutions and permutations
- Two main techniques
  - **Feistel network** or Feistel scheme
  - **substitution-permutation networks** (SPN network)

Block ciphers

- Block cipher
  - deterministic algorithm
  - operates on fixed-length groups of bits, called **blocks**,
  - an unvarying transformation specified by a **symmetric key**.
- Design of block ciphers
  - based on the concept of an **iterated product cipher**
  - suggested and analyzed by Claude Shannon
  - by combining simple operations such as substitutions and permutations
- Two main techniques
  - **Feistel network** or Feistel scheme
  - **substitution-permutation networks** (SPN network)

Block ciphers - Definition

Problem: the plaintexts may be extremally long

$\rightsquigarrow$ hard to analyse security of the cipher.

Idea: Design ciphers that work on small blocks ...

two paired algorithms

- one for encryption $\mathcal{E}$
- one for decryption $\mathcal{D}$

that accept two inputs:

- an input block of size n bits
- a key of size k bits

$$\begin{aligned} \mathcal{E}_K(P) &:= \mathcal{E}(K,P) : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n \\ \mathcal{E}_K^{-1}(C) &:= \mathcal{D}_K(C) = \mathcal{D}(K,C) : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n \end{aligned}$$

$$\boxed{\forall K, \forall P : \mathcal{D}_K(\mathcal{E}_K(P)) = P}$$

Block ciphers - Definition

Problem: the plaintexts may be extremally long

$\rightsquigarrow$ hard to analyse security of the cipher.

Idea: Design ciphers that work on small blocks ...

two paired algorithms

- one for encryption $\mathcal{E}$
- one for decryption $\mathcal{D}$

that accept two inputs:

- an input block of size n bits
- a key of size k bits

$$\begin{aligned} \mathcal{E}_K(P) &:= \mathcal{E}(K,P) : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n \\ \mathcal{E}_K^{-1}(C) &:= \mathcal{D}_K(C) = \mathcal{D}(K,C) : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n \end{aligned}$$

$$\boxed{\forall K, \forall P : \mathcal{D}_K(\mathcal{E}_K(P)) = P}$$

Block ciphers - Definition

Problem: the plaintexts may be extremally long

$\rightsquigarrow$ hard to analyse security of the cipher.

Idea: Design ciphers that work on small blocks ...

two paired algorithms

- one for encryption $\mathcal{E}$
- one for decryption $\mathcal{D}$

that accept two inputs:

- an input block of size n bits
- a key of size k bits

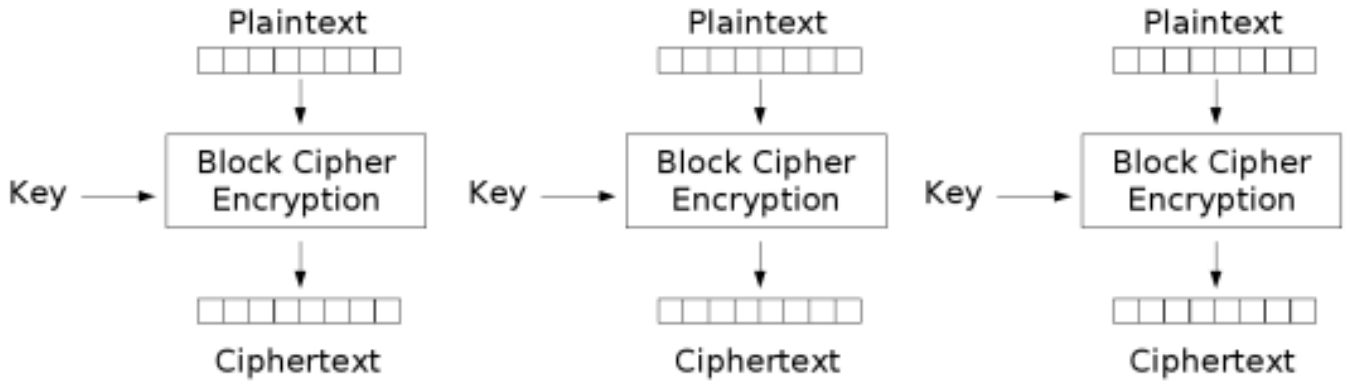
$$\begin{aligned} \mathcal{E}_K(P) &:= \mathcal{E}(K,P) : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n \\ \mathcal{E}_K^{-1}(C) &:= \mathcal{D}_K(C) = \mathcal{D}(K,C) : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n \end{aligned}$$

$$\boxed{\forall K, \forall P : \mathcal{D}_K(\mathcal{E}_K(P)) = P}$$

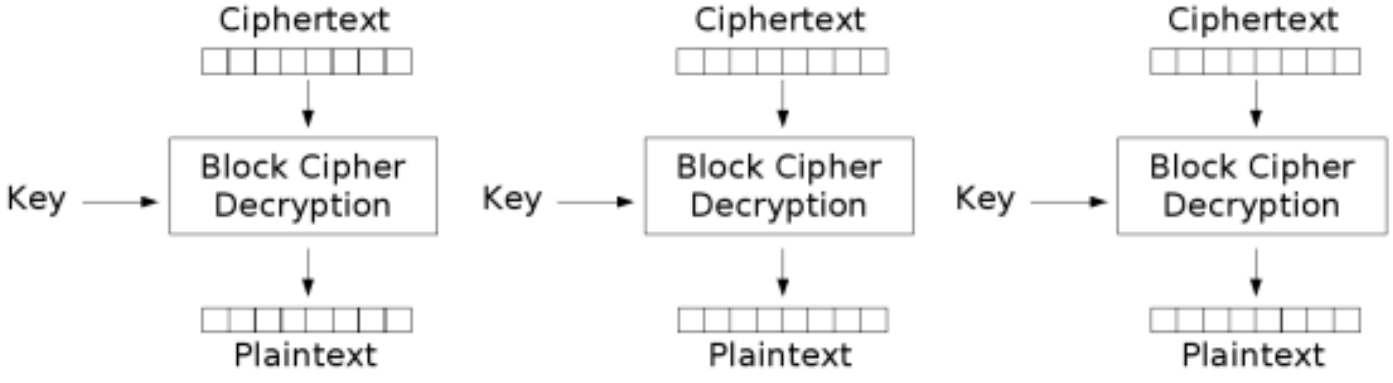
Mode of operations

- Block ciphers cannot be used **directly** for encryption.
- They are always used in some "modes of operation"
  - Electronic Codebook (ECB) mode
  - Cipher-Block Chaining (CBC) mode,
  - Output Feedback (OFB) mode,
  - Counter (CTR) mode,
  - ...

Electronic codebook (ECB)

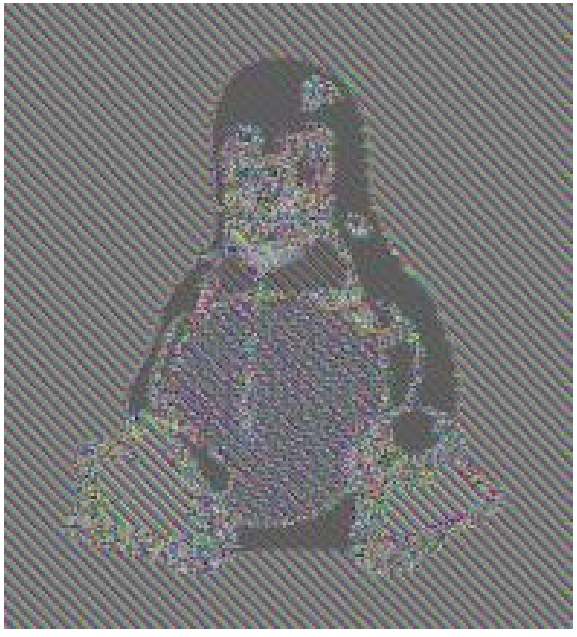


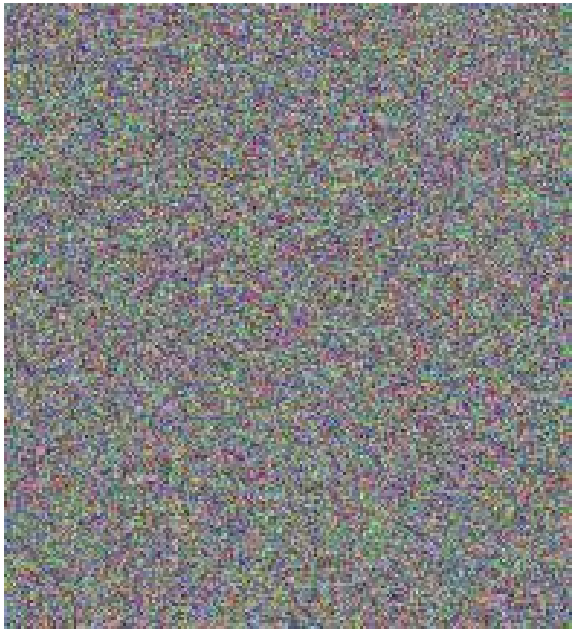
Electronic Codebook (ECB) mode encryption



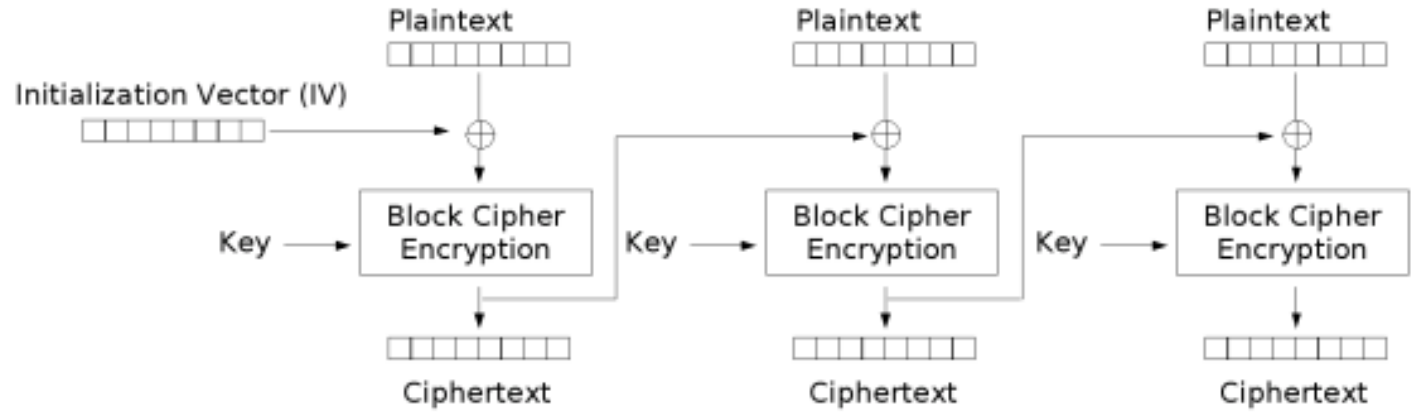
Electronic Codebook (ECB) mode decryption

Electronic codebook (ECB) should not be used !

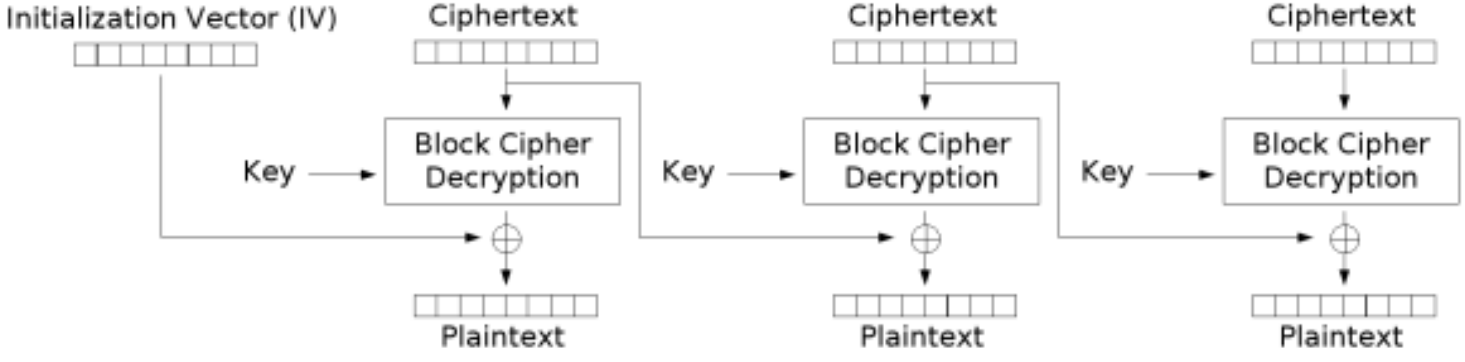




Cipher-block chaining (CBC)



Cipher Block Chaining (CBC) mode encryption



Cipher Block Chaining (CBC) mode decryption

Cipher-block chaining (CBC)

- **Error propagation?**

Error in block c_i affects only m_i and m_{i+1}
$\rightsquigarrow$ errors do not propagate

- **Can encryption be parallelized?**

No !

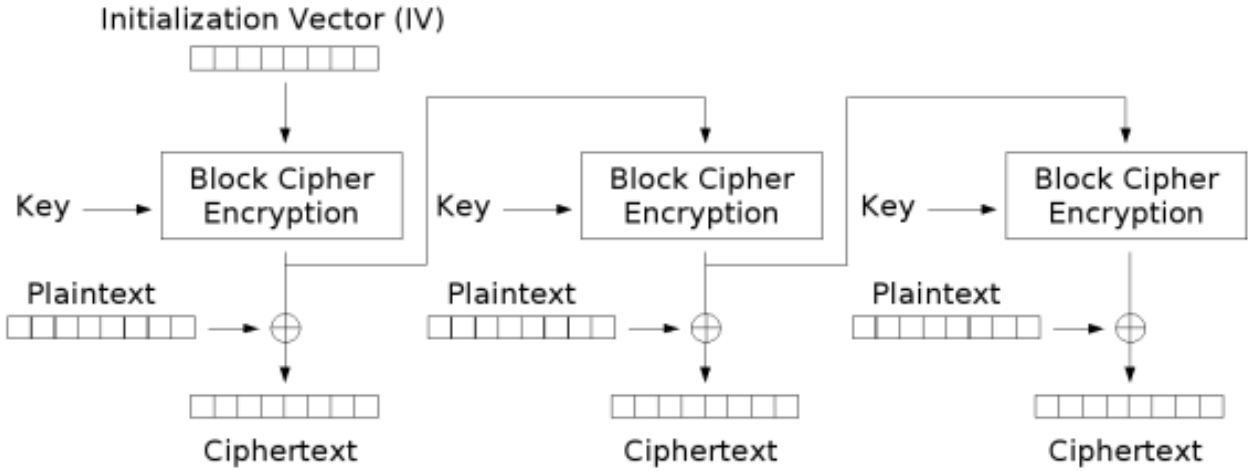
- **Can decryption be parallelized?**

Yes !

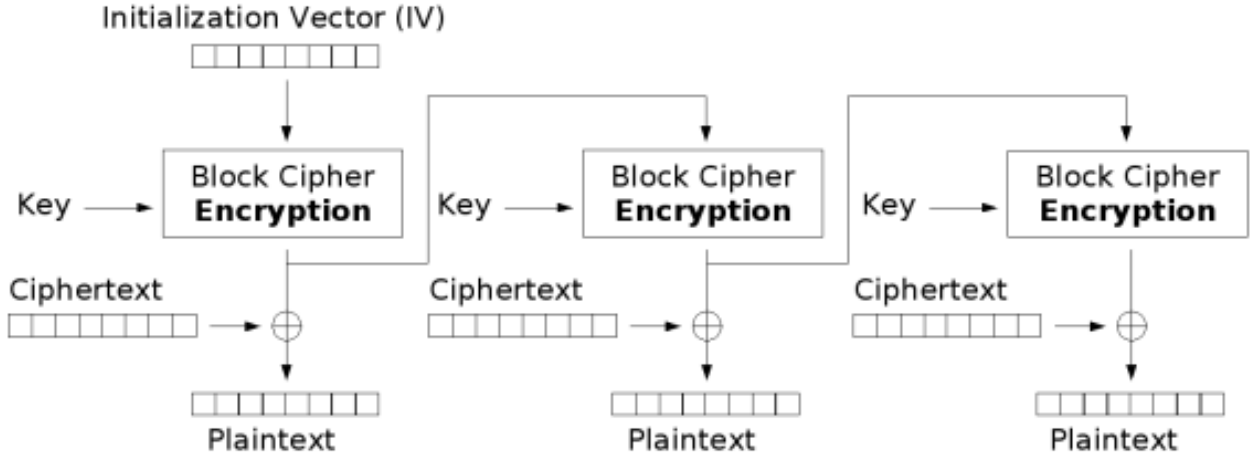
- **What if one bit of plaintext is changed (somewhere at the beginning)?**

Everything needs to be recomputed
(not so good e.g. for disc encryption)

Output feedback (OFB)



Output Feedback (OFB) mode encryption



Output Feedback (OFB) mode decryption

Output feedback (OFB)

- **Error propagation?**

Error in block c_i affects only m_i and m_{i+1}
$\rightsquigarrow$ errors do not propagate

- **Can encryption/decryption be parallelized?**

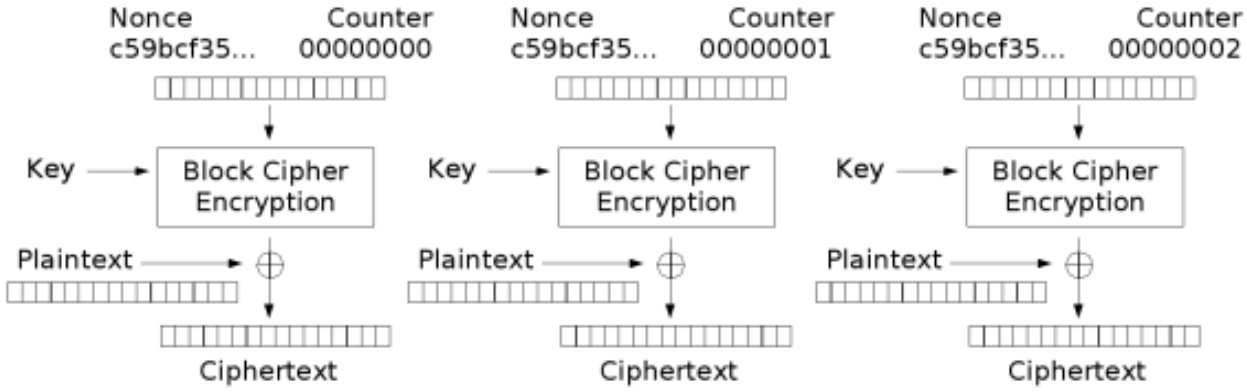
No ! ...

...but we can we can use precomputation

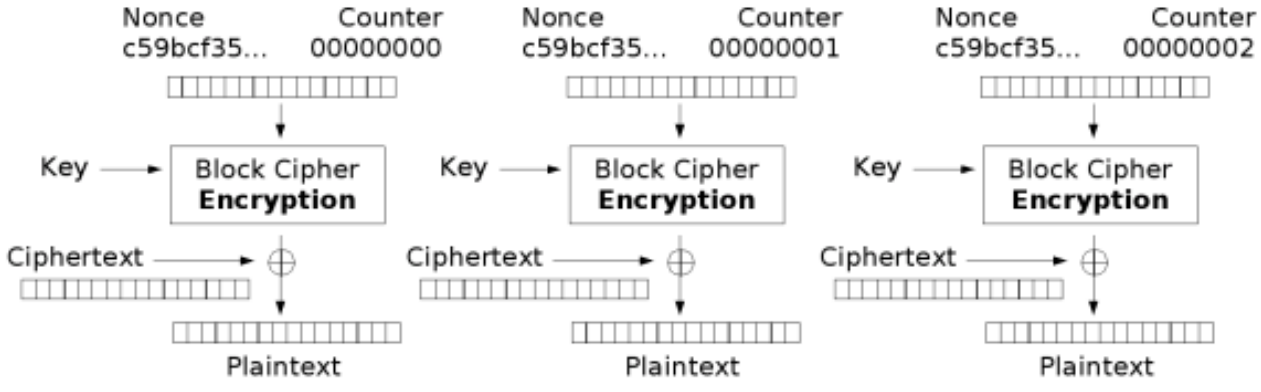
- **What if one bit of plaintext is changed (somewhere at the beginning)?**

Only one block needs to be recomputed

Counter (CTR)



Counter (CTR) mode encryption



Counter (CTR) mode decryption

Counter (CTR)

- **Error propagation?**

Error in block c_i affects only c_i and c_{i+1}
$\rightsquigarrow$ errors do not propagate

- **Can encryption/decryption be parallelized?**

Yes ! ...

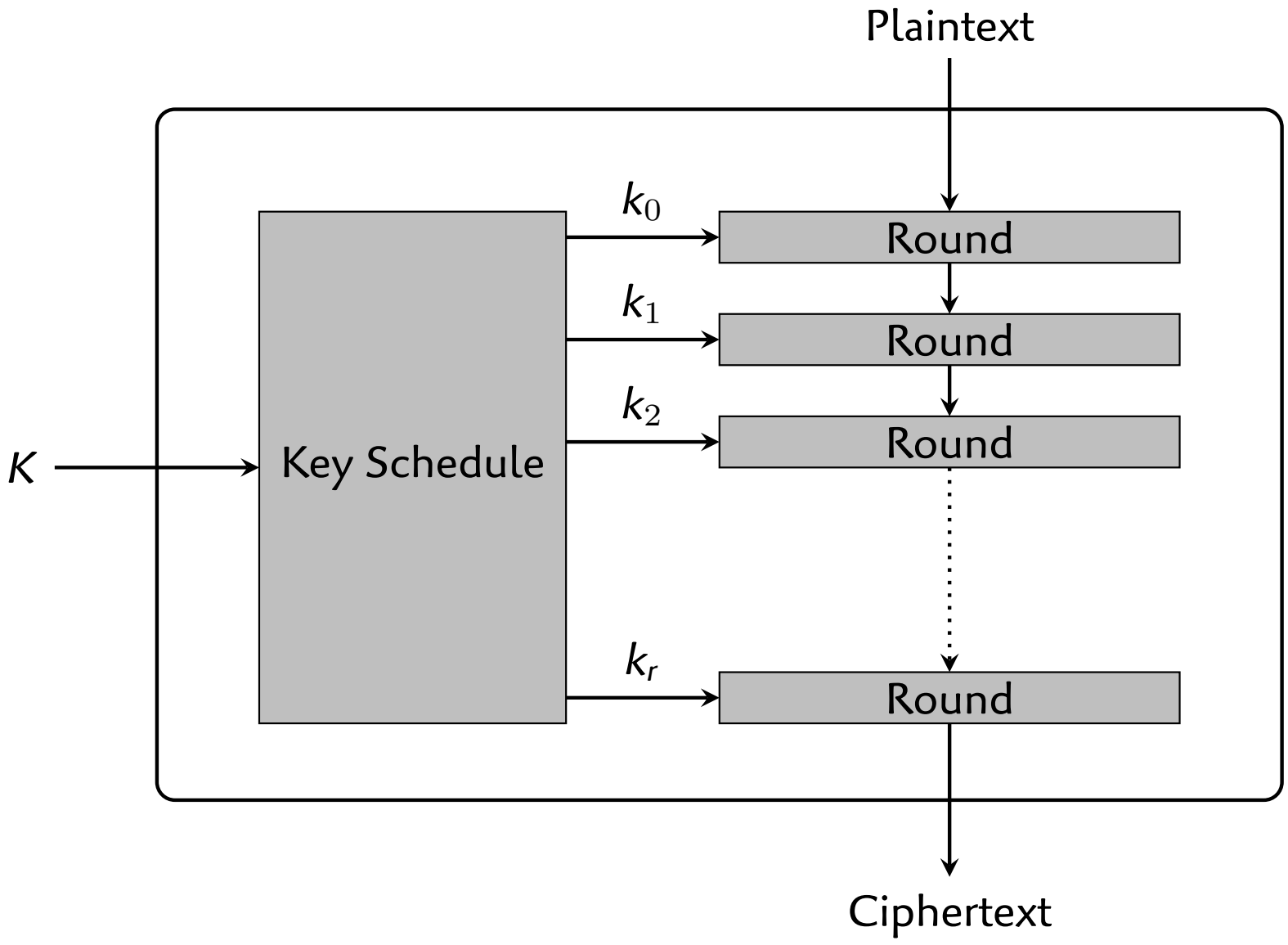
...and we can we can use precomputation

possible to decrypt one block without decrypting anything else

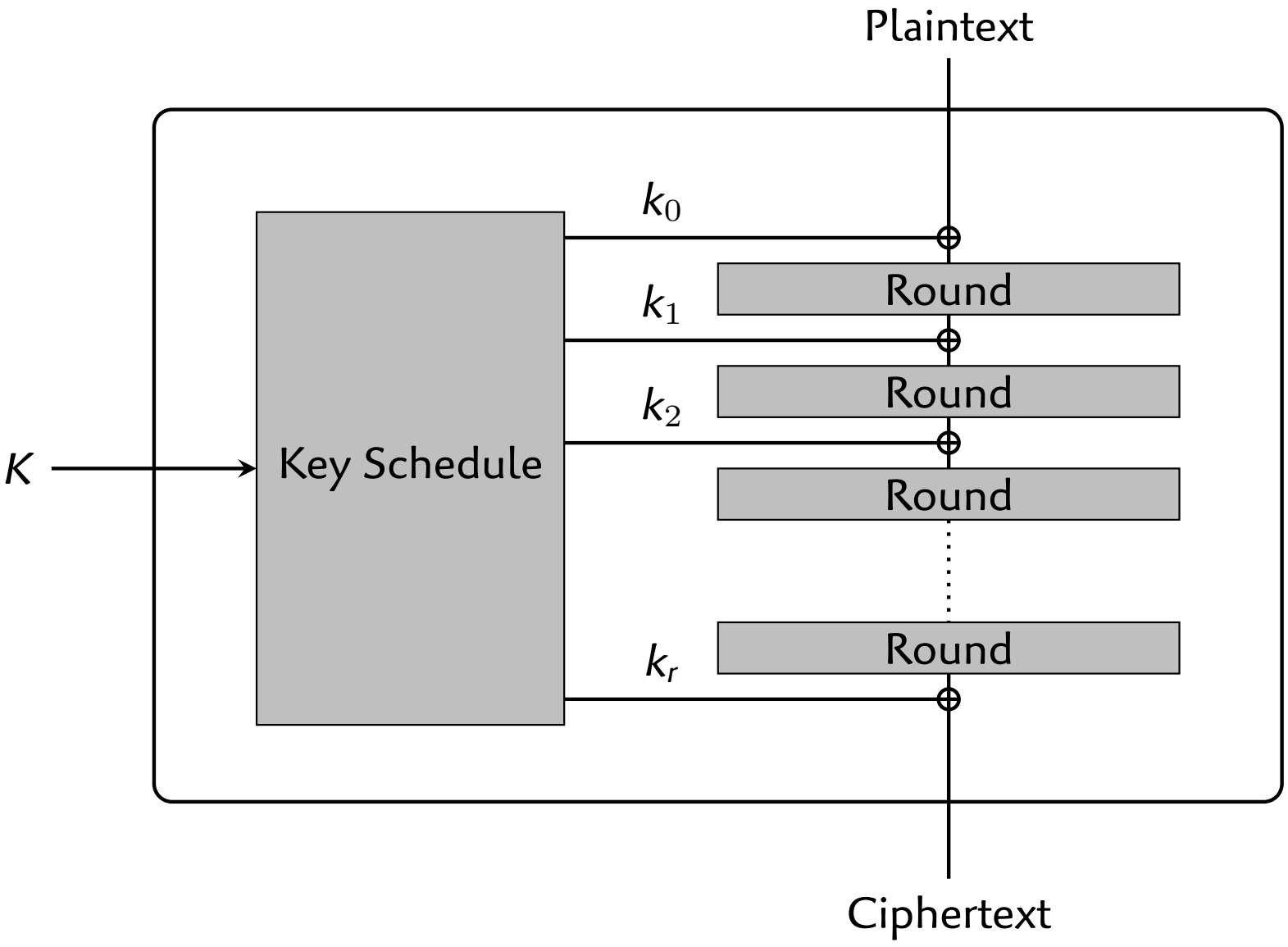
- **What if one bit of plaintext is changed (somewhere at the beginning)?**

Only one block needs to be recomputed

Block Ciphers: Iterated Structure



Block Ciphers: Iterated Structure



Mécanisme de chiffrement symétrique

Block Cipher

$$\mathcal{E}_K(P) : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$$
$$\mathcal{D}_K(C) : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$$

(Symmetric) Encryption Scheme

$$\mathcal{E}_K(P) : \{0,1\}^k \times \{0,1\}^* \to \{0,1\}^*$$
$$\mathcal{D}_K(C) : \{0,1\}^k \times \{0,1\}^* \to \{0,1\}^* \cup \{\perp\}$$

$$\forall K, \forall P : \mathcal{D}_K(\mathcal{E}_K(P)) = P$$

Authenticated encryption $\approx$ knowledge of K is **necessary** to produce a valid ciphertext

Data Encryption Standard (DES)

- First version designed by IBM in 1973-74, based on a **Lucifer cipher** (by Horst Feistel).
- **National Security Agency** (NSA) played some (unclear ...) role in the design of DES.
- made public in 1975.
- approved as a US federal standard in November 1976.

- Key length:
  - effective: 56 bits
  - **formally:** 64 bits (8 bits for checking parity).
- Block length: 64 bits

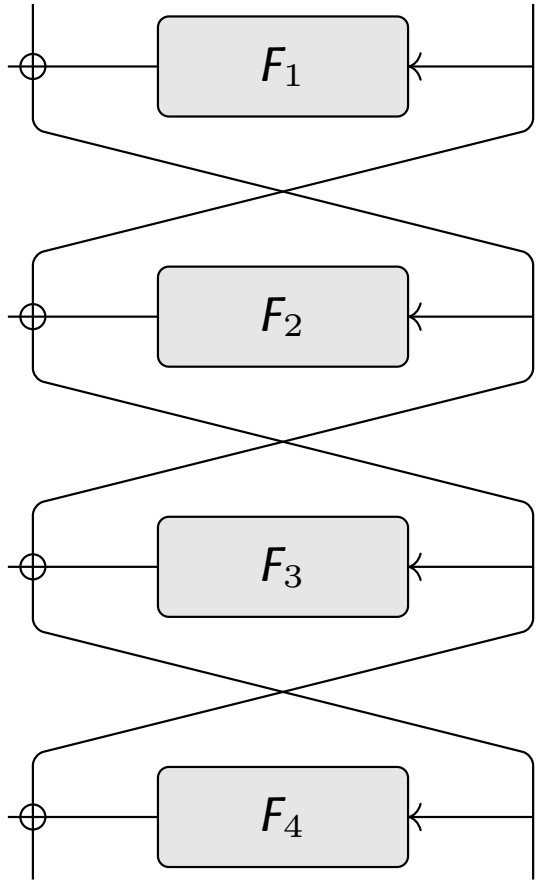
Data Encryption Standard (DES)

- First version designed by IBM in 1973-74, based on a **Lucifer cipher** (by Horst Feistel).
- **National Security Agency** (NSA) played some (unclear ...) role in the design of DES.
- made public in 1975.
- approved as a US federal standard in November 1976.

- Key length:
  - effective: 56 bits
  - **formally:** 64 bits (8 bits for checking parity).
- Block length: 64 bits

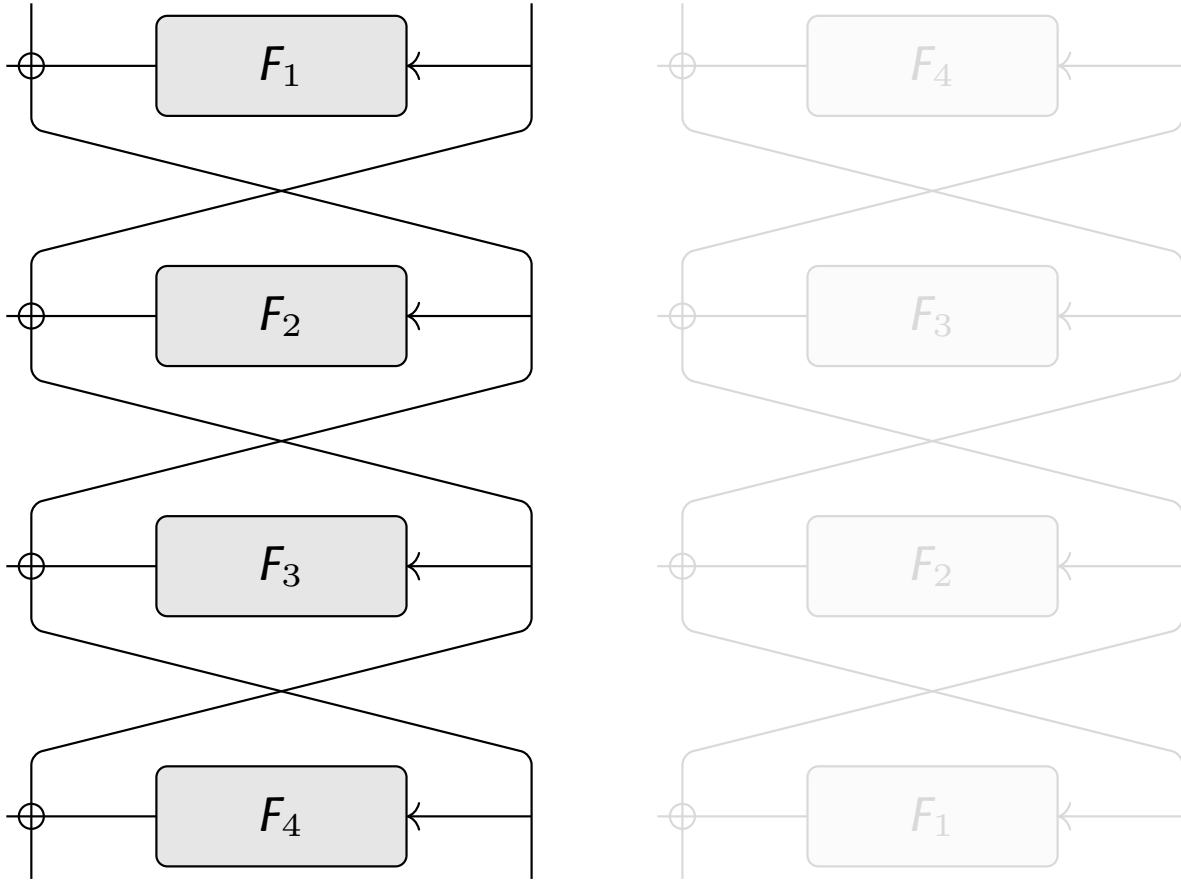
Feistel Scheme

- symmetric structure used in the construction of block ciphers
- invented by cryptographer Horst Feistel



Feistel Scheme

- invertible !



Feistel Scheme

- invertible !