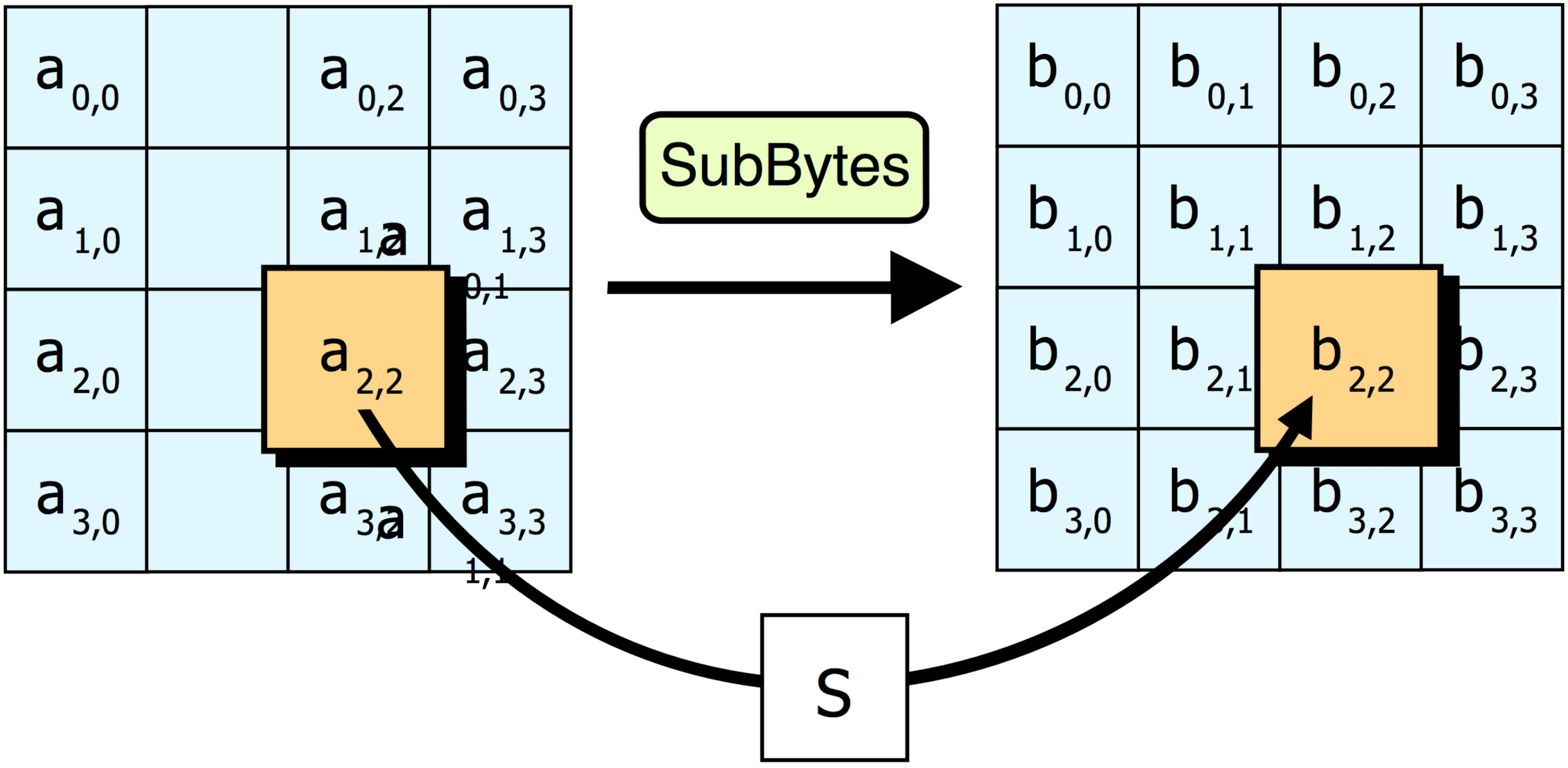


Session 3
Chiffrement par Bloc

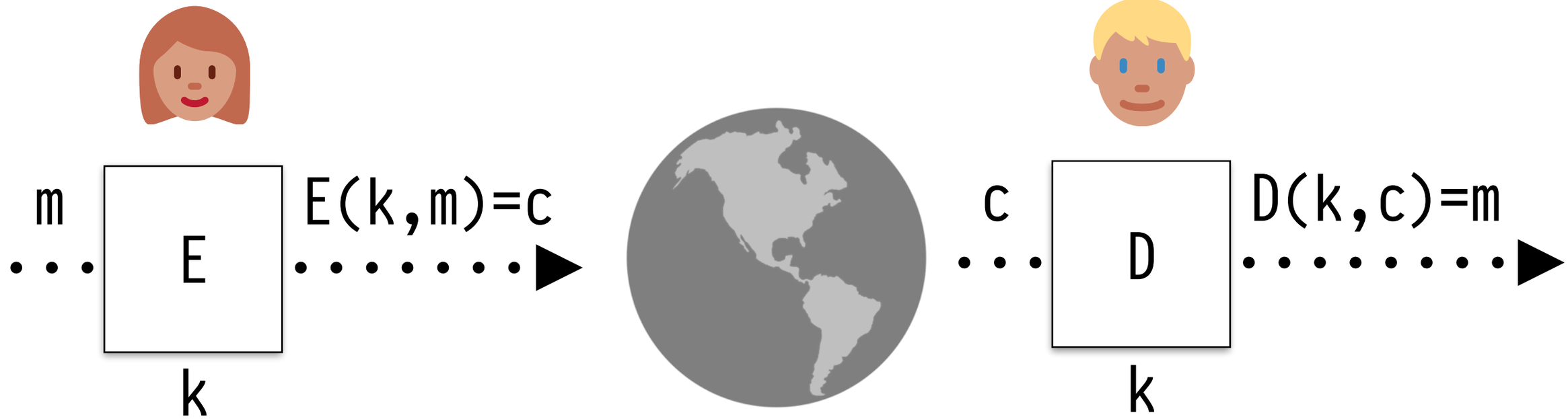
Introduction à la Cryptographie

Nadim Kobeissi

Chiffrement par Bloc

- Méthode de chiffrement d'un texte, utilisant une clé.
- La taille du texte et de la clé sont **fixes** et divisés en *blocs*.
- Cela permet plus de contrôle sur le propriétés du chiffrement.
- Cette session est pratique — le cours prochain sera un traitement plus théorique des chiffrements par bloc.

Rappel: Chiffrement Symétrique



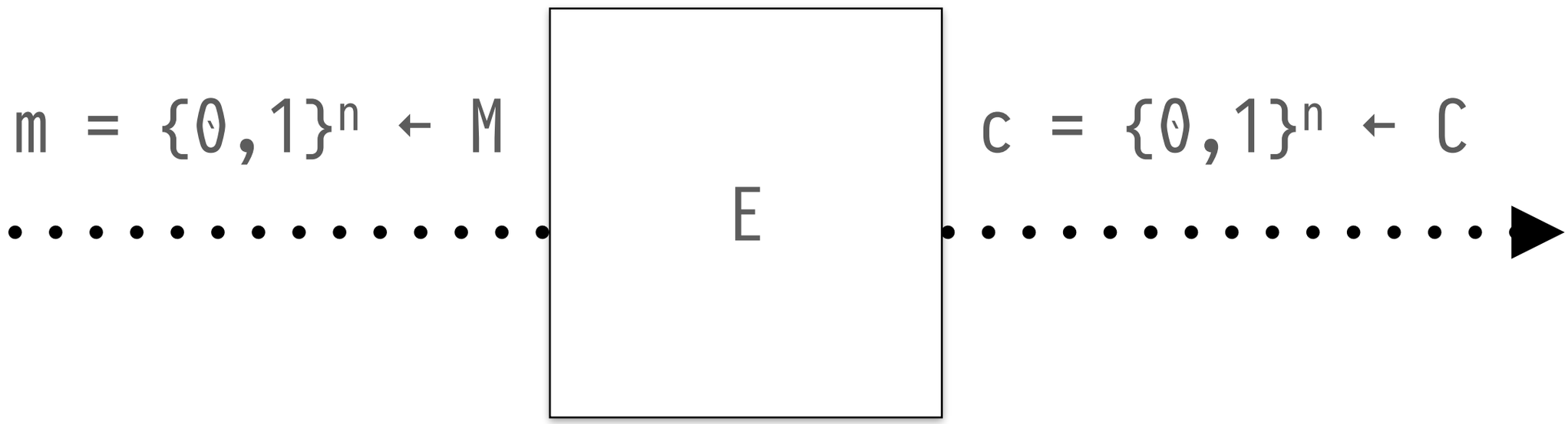
Pas d'espionnage,
Pas d'alteration.

m: Message, k: Clé
E, D: Fonctions de chiffrement (connus)
c: Message chiffré

E et D sont *efficaces, inversibles*.

m, k, et c sont de taille déterminée!

Un Regard Plus Proche

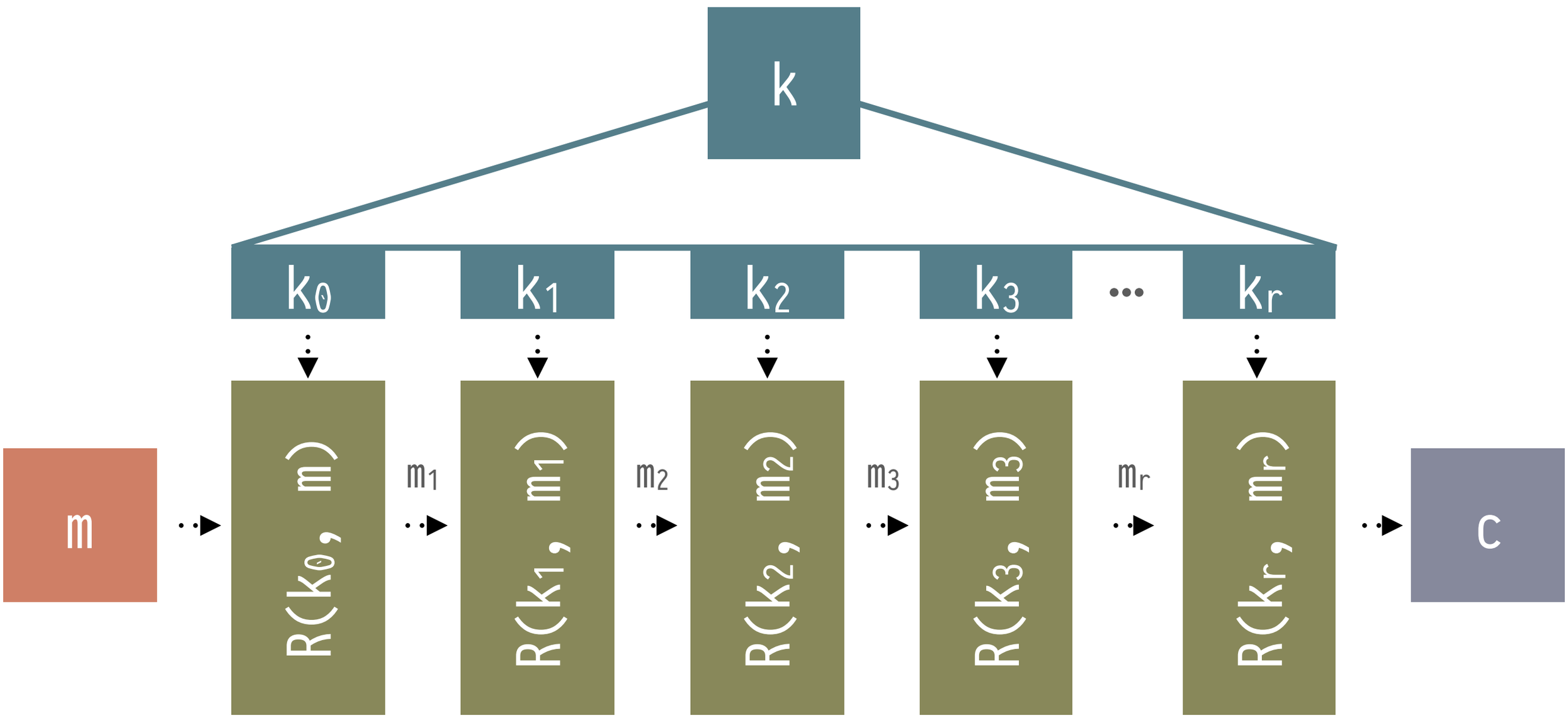


$k = \{0,1\}^x \leftarrow K$

Exemples:

- 3DES: n = 64, x = 168
- AES: n = 128, x = 128, 192, 256

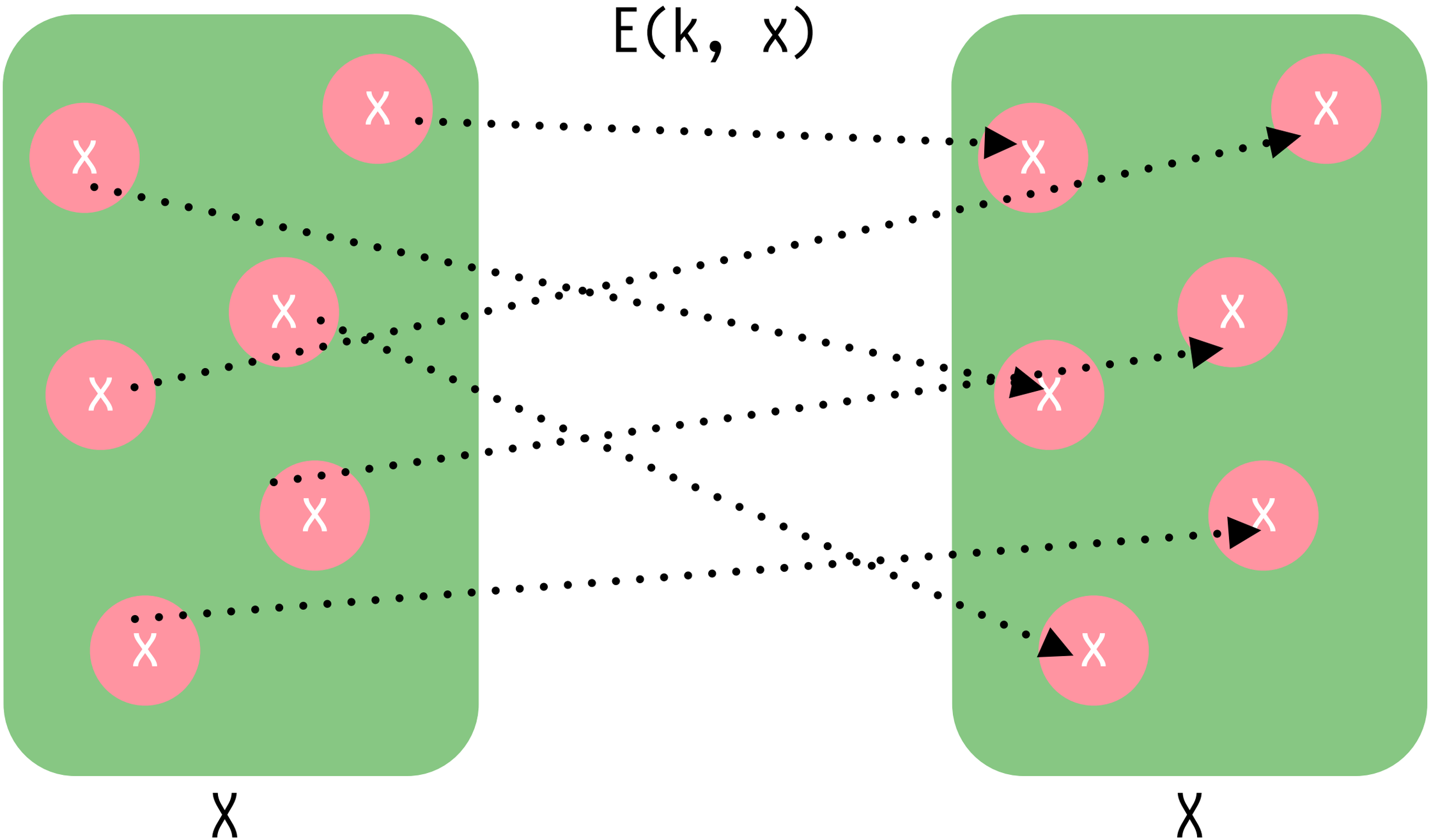
Chiffrement par Bloc: Bâtit En Serie



Fonctions Aléatoires: Toujours Notre But

- `X(U)` $\longrightarrow$ `V`
- Exemple: `X(U,I)` $\longrightarrow$ `V`
- *Nouvelle definition!* Permutation Aléatoire:
  - `E(K,X)` $\longrightarrow$ `X`, tel que:
    - Il existe une façon “efficace” de évaluer cette permutation.
    - Il existe un algorithme d’inversion `D(K,Y)` “efficace” aussi.
    - La fonction `E(K,·)` est une fonction “one-to-one” (bijection)

Bijection (fonction “one-to-one”)



AES et DES Sont Des Permutations Aléatoires!

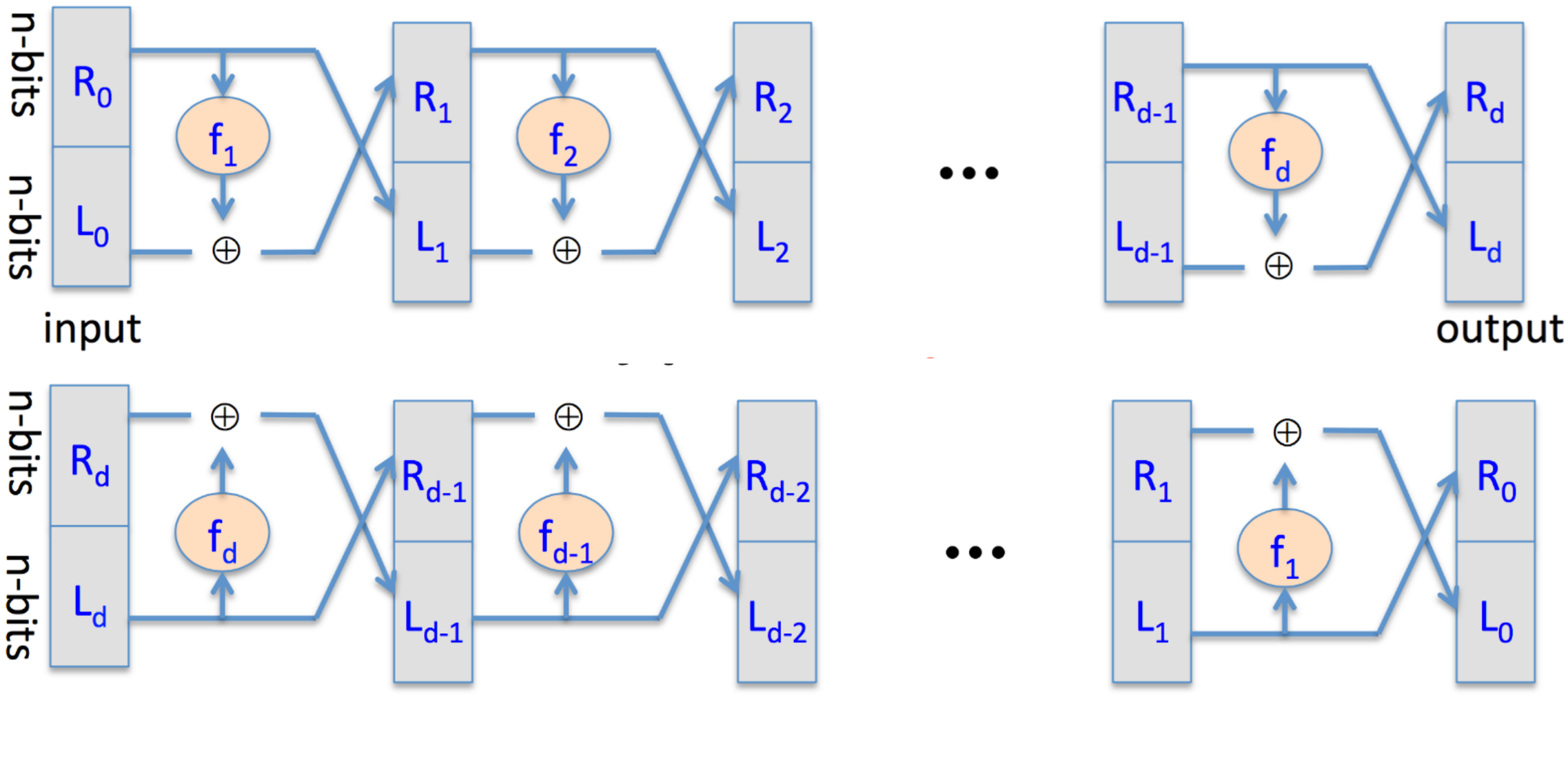
- AES: $E(K, X) \longrightarrow X$ ou $K = X = \{0,1\}^{128}$
- 3DES: $E(K, X) \longrightarrow X$ ou $K = \{0,1\}^{168}$, $X = \{0,1\}^{64}$
- Fonctionnellement, toutes les permutations aléatoires sont des fonctions aléatoires.

DES: Data Encryption Standard

- 1970: Horst Feistel (IBM) invente le chiffrement par bloc “Lucifer”. $k = \{0,1\}^{128}$, $m = \{0,1\}^{128}$
- 1973: Le Bureau National des Standards Américains demande des propositions de standard national pour le chiffrement de bloc.
- 1976: Le DES, un variant de Lucifer, est adopté comme ce standard. $k = \{0,1\}^{56}$, $m = \{0,1\}^{64}$
- 1997: DES cassé par la recherche exhaustive (AES en 2000.)

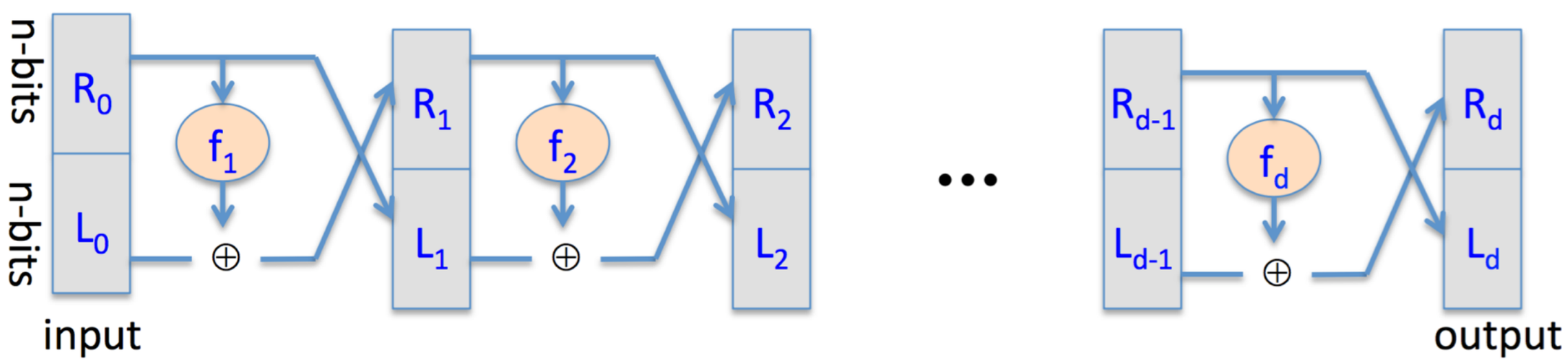
DES: Idée de Base: Réseaux Feistel

- Comment appliquer des fonctions façon que le résultat soit reversible?

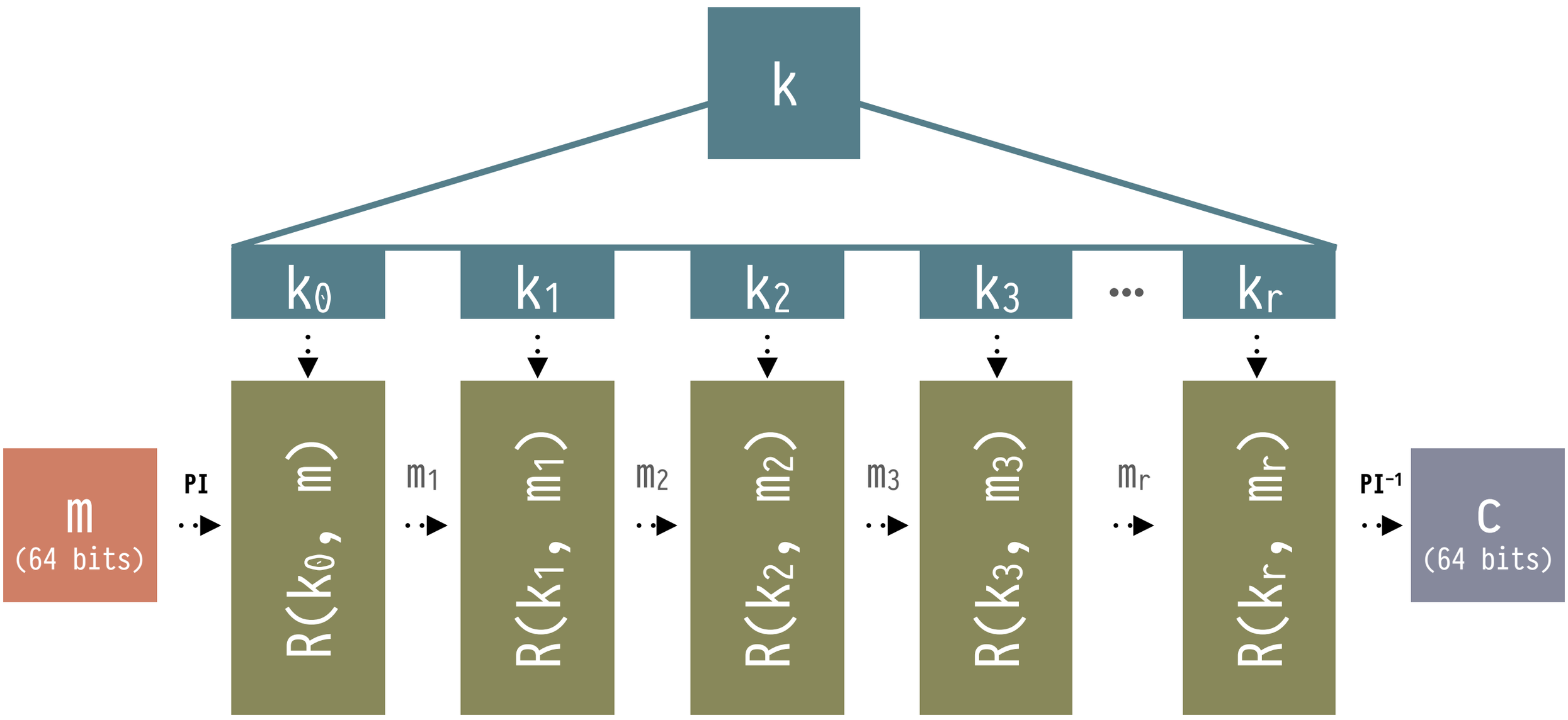


Théorème de Sécurité des Réseaux Feistel

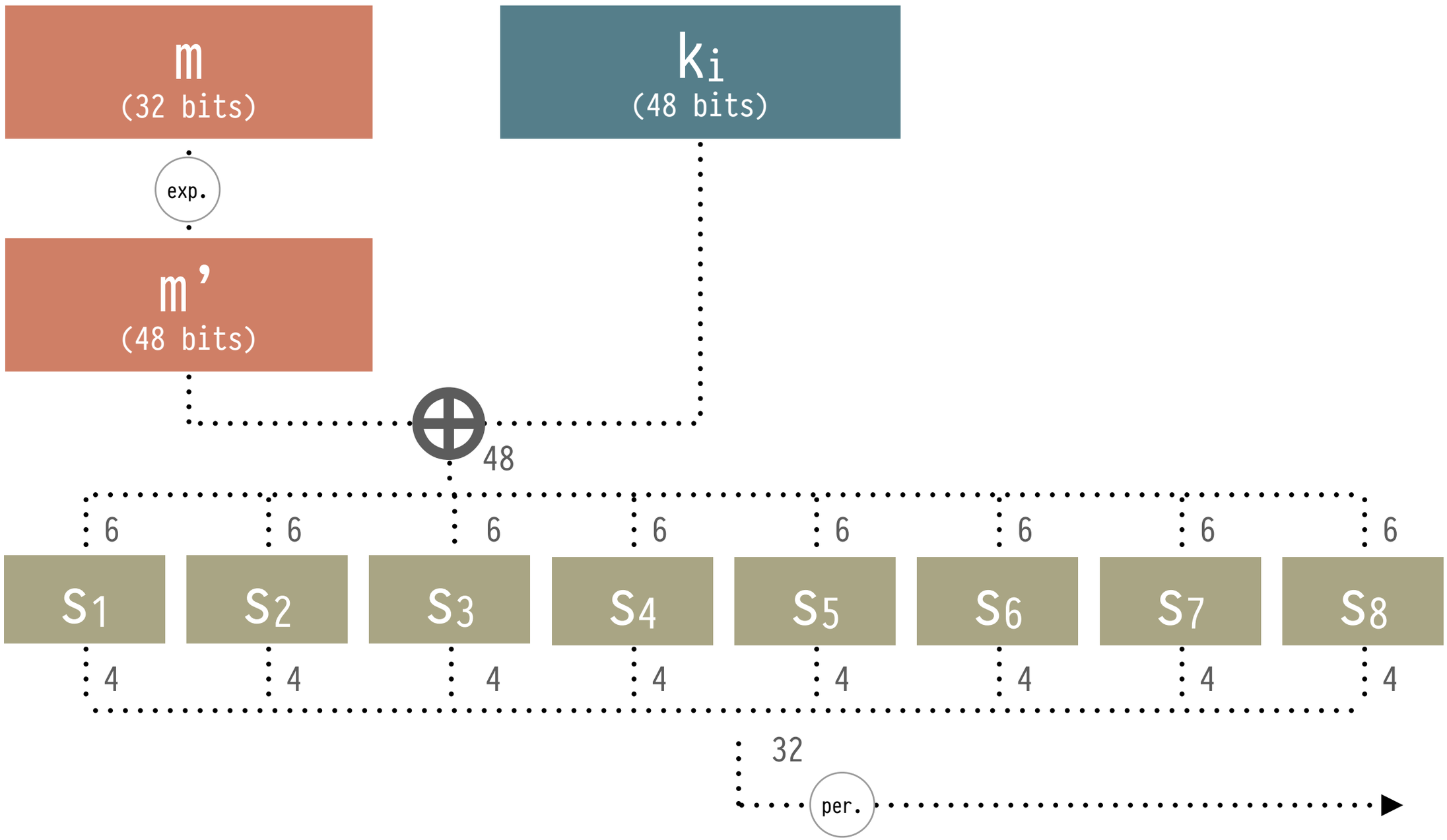
- Si une fonction aléatoire sûre est utilisée pour trois cycles Feistel avec trois clés indépendants, on obtient une permutation aléatoire sure. (Ruby-Lackoff, 1985).



DES: Un Réseau Feistel de 16 Cycles



La Fonction dans Chaque Cycle Feistel F(k_i, m)



Un S-Box DES

- La boite de substitutions (“S-box”) se charge de substituer l’input pour la valeur la plus indépendante mathématiquement, non-linéaire, non-affine.

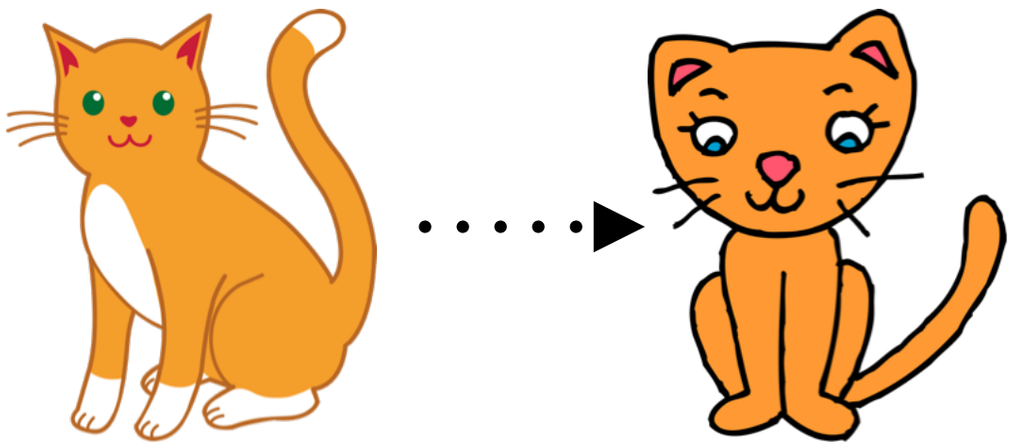
S_5		Middle 4 bits of input															
		0000	**0001**	**0010**	**0011**	**0100**	**0101**	**0110**	**0111**	**1000**	**1001**	**1010**	**1011**	**1100**	**1101**	**1110**	**1111**
Outer bits	**00**	0010	1100	0100	0001	0111	1010	1011	0110	1000	0101	0011	1111	1101	0000	1110	1001
	01	1110	1011	0010	1100	0100	0111	1101	0001	0101	0000	1111	1010	0011	1001	1000	0110
	10	0100	0010	0001	1011	1010	1101	0111	1000	1111	1001	1100	0101	0110	0011	0000	1110
	11	1011	1000	1100	0111	0001	1110	0010	1101	0110	1111	0000	1001	1010	0100	0101	0011

$$011011 \longrightarrow 1001$$

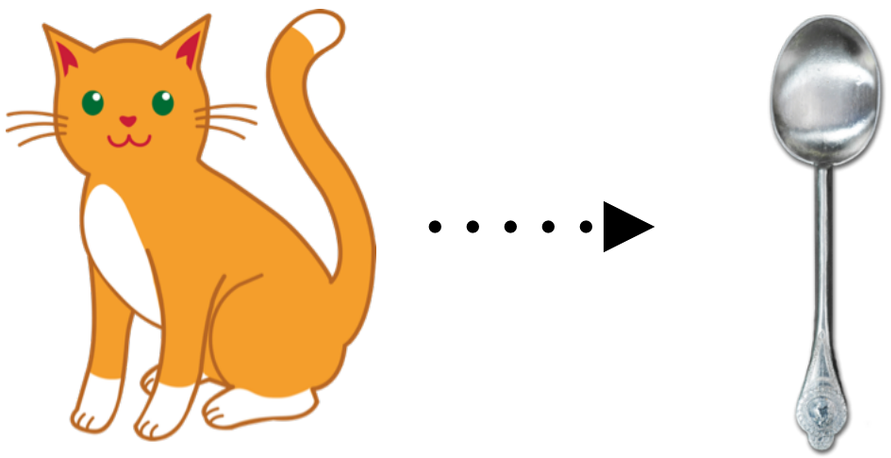
L’Importance des S-Box

- Un DES sans S-Box est simplement une fonction XOR/ permutations linéaires. Aucune sécurité.

- Les fonctions linéaires peuvent être prédites, reversées et transformées d’une façon algorithmique.



Mauvais S-Box



Bon S-Box

Critères d'un S-Box Sûr

- Publiées officiellement en 1994.
- Aucune transformation doit être "proche" a une transformation linéaire ou affine.
- La distribution doit être uniforme.
- Autres critères liées.
- Critères indiquent que les auteurs connaissaient déjà des techniques de cryptanalyse pas encore inventés (différentielle, inventée 10 ans plus tard.)

Design criteria

We list here the criteria tor the S-boxes and the permutation P, which were used in the original specifications, and which are satisfied by the design of DES.

The relevant criteria for the S-boxes are as follows:

(S-1) Each S-box has six bits of input and four bits of output. (This was the largest size that we could accommodate and still fit all of DES onto a single chip in 1974 technology.)

(S-2) No output bit of an S-box should be too close to a linear function of the input bits. (That is, if we select any output bit position and any subset of the six input bit positions, the fraction of inputs for which this output bit equals the XOR of these input bits should not be close to 0 or 1, but rather should be near 1/2.)

(S-3) If we fix the leftmost and rightmost input bits of the S-box and vary the four middle bits, each possible 4-bit output is attained exactly once as the middle four input bits range over their 16 possibilities.

(S-4) If two inputs to an S-box differ in exactly one bit, the outputs must differ in at least two bits. (That is, if $|\Delta I_{i,j}| = 1$, then $|\Delta O_{i,j}| \geq 2$, where $|x|$ is the number of 1-bits in the quantity x.)

Attaque: La Recherche Exhaustive

- **But:** Sachant quelques pairs de inputs/outputs:
  - $(m_i, c_i = E(k, m_i))$, trouver la clé k.
- Si DES est vraiment un *chiffrement ideal*, il doit exister une clé dans l'espace de taille 2^{56} qui permet l'inversion d'une permutation aléatoire qui a produit un chiffrement.
- Plus simple: On essaye tout les 2^{56} clés possible, quoi.

Attaque: La Recherche Exhaustive

- Le “DES Challenge”:
  - m = “The unknown message is: xxxxxxx”
  - c = c_1, c_2, c_3, c_4
- Trouver $k \in \{0,1\}^{56}$ tel que $DES(k, m_i) = c_i$ pour $i=1,2,3$
  - 1997 — Recherche Internet: 3 mois.
  - 1998 — Le “Deep Crack” de EFF: 3 jours.

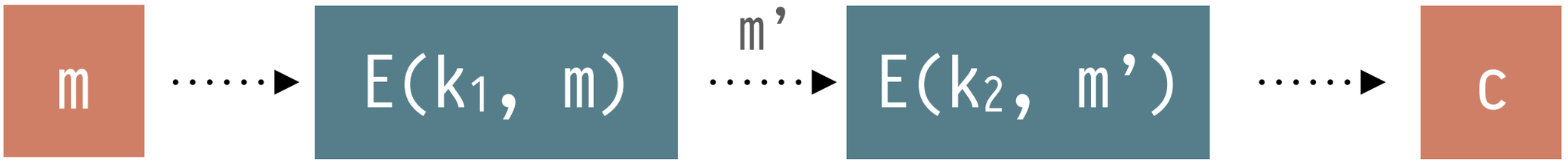
Protéger DES Contre la Recherche Exhaustive

- Une methode: **Triple DES (3DES)**:
  - $E(K, M) \longrightarrow M$ est un chiffrement par bloc.
  - $\mathbf{3E}(K^3 \times M \longrightarrow M)$ est defini tel que:
    - $\mathbf{3E}((k_1, k_2, k_3), m) = E(k_1, D(k_2, E(k_3, m)))$
- 3DES: trois fois moins rapide, mais $|K| = 2^{(56*3=168)}$.

(Attaque connue en 2^{118})

Pourquoi Pas Double DES?

- Chiffrons deux fois avec deux clés indépendants:



- Question: Quelle est la taille de l'espace des clés avec 2DES (pour DES = 2^{56}, 3DES = 2^{168})?

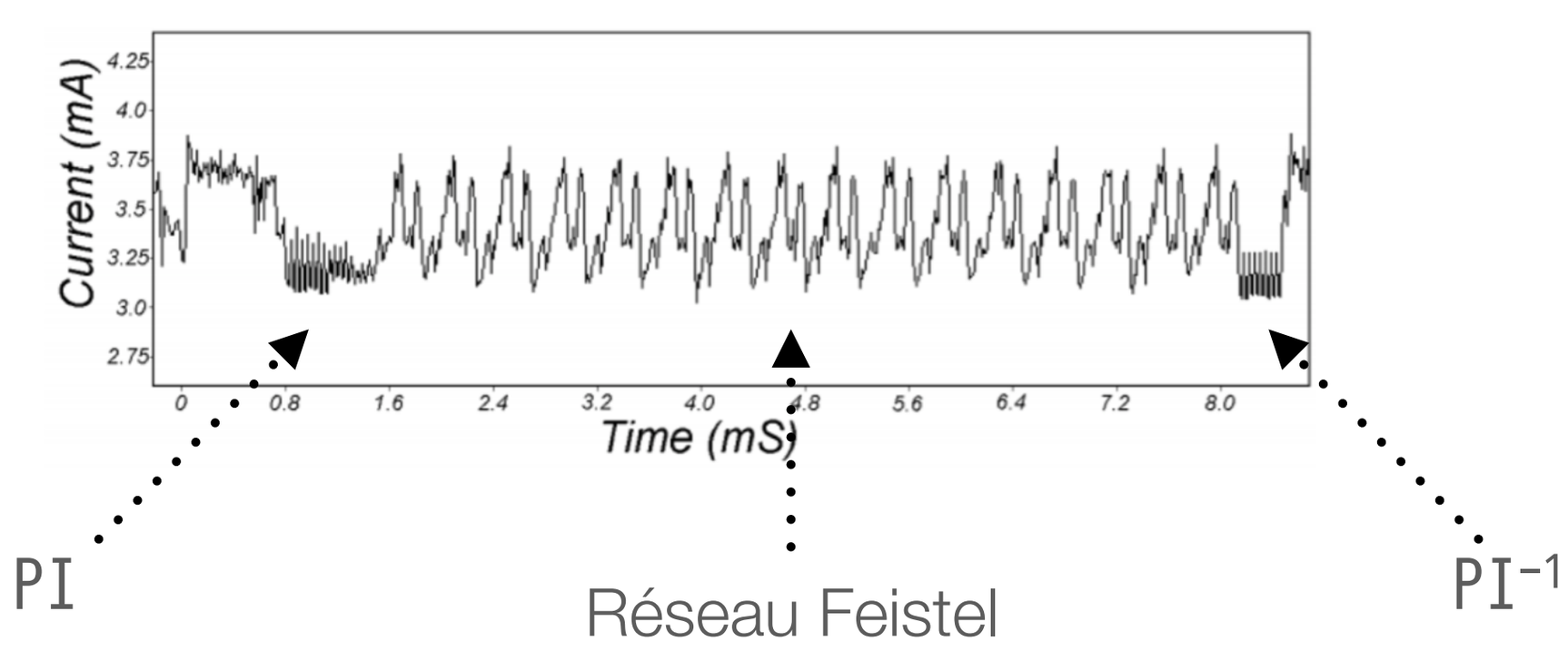
2^{57}

- $E(k_1, m) = m' = D(k_2, c)$

- On bâtit une table de la premiere operation, et on compare les résultats a la deuxième operation.

Attaques Pratiques et “Side-Channels”

- Analyse de puissance du courant.
- Si les operations sont différents en utilisation de courant, de RAM, de CPU… ont peut les profiler.



AES: Advanced Encryption Standard (2000)

- 1997: NIST publie une demande de propositions.
- 1998: Quinze propositions des universités tout autour le monde.
- 1999: NIST choisit 5 finalistes.
- 2000: NIST choisit Rijndael pour être le AES (conçu a Lausanne, Belgique, par Vincent Rijmen et Joan Daemen).

	Rijndael	Serpent	Twofish	MARS	RC6
General Security	2	3	3	3	2
Implementation Difficulty	3	3	2	1	1
Software Performance	3	1	1	2	2
Smart Card Performance	3	3	2	1	1
Hardware Performance	3	3	2	1	2
Design Features	2	1	3	2	1
~~Total~~	16	14	13	10	9

AES: Advanced Encryption Standard (2000)

- On va regarder une animation qui explique comment marche AES!

- Pour ceux qui téléchargent ces slides en ligne, trouvez l'animation sur le GitHub. Elle est en Adobe Flash.

Les Prochains Cours

- Et si on veut chiffrer plusieurs blocs?
- Comment faire pour l'authentification?
- Quelles sont des autres attaques?
- Et plus de théorie et de descriptions formelles!

Suivez le Cours En Ligne

- http://courscrypto.org
  - Matériaux.
  - Devoirs/TPs.
  - Slides et vidéos.
  - A la semaine prochaine!

Je conseille vivement lire ce livre