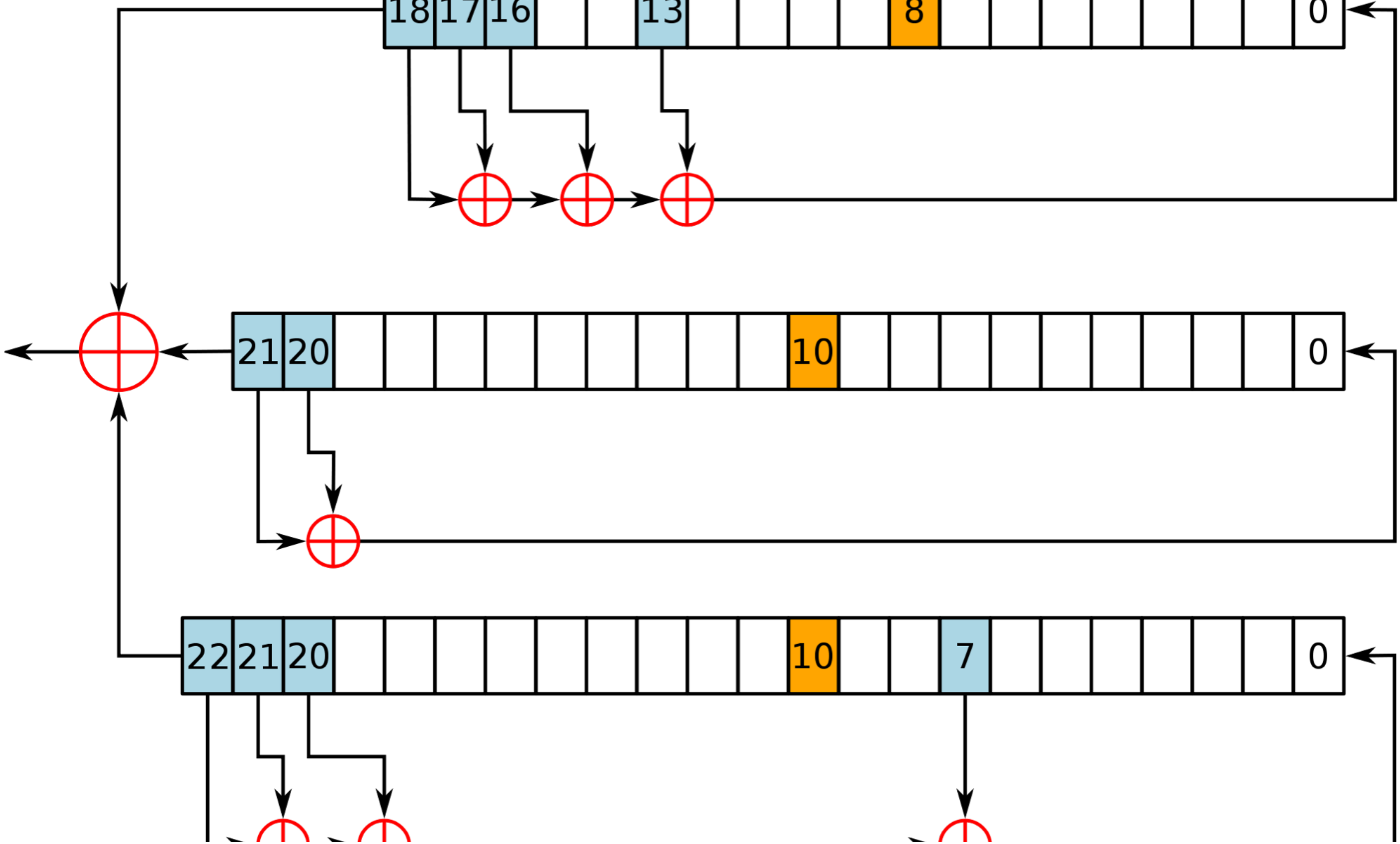


Session 2
Chiffrement de Flux

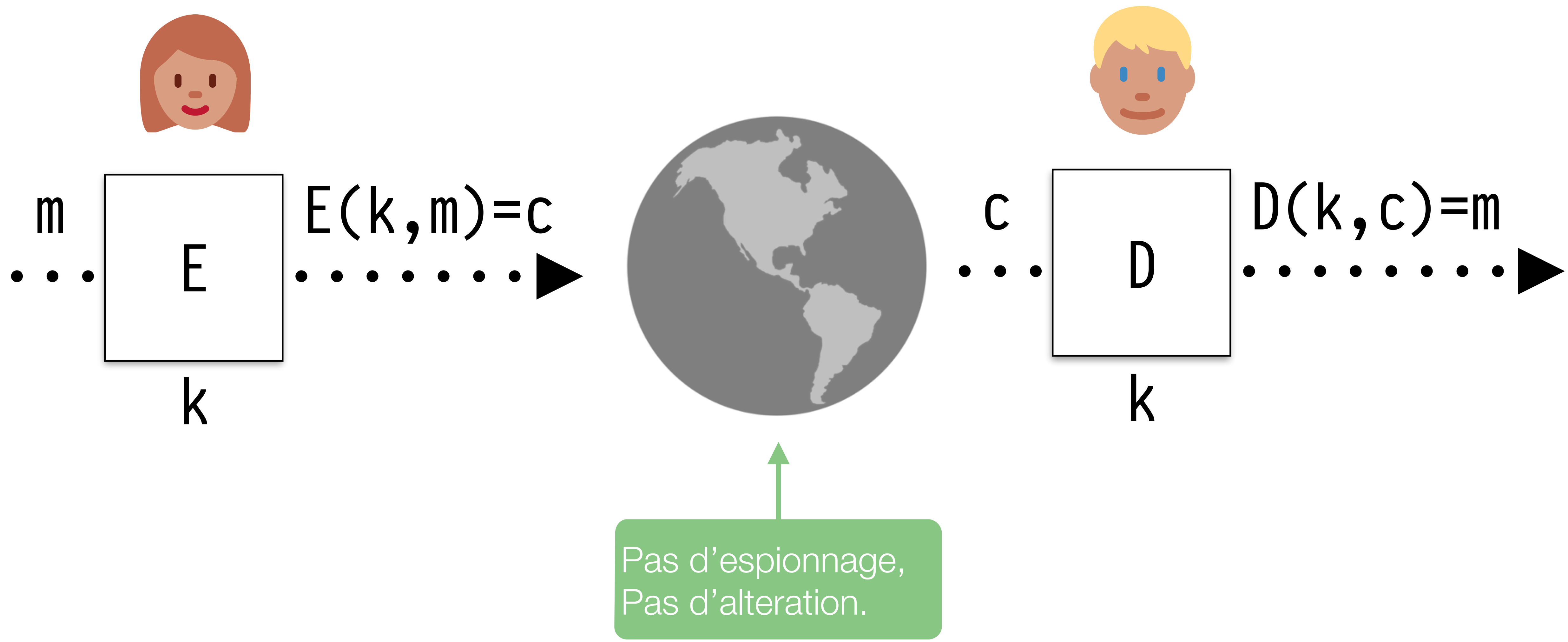
Introduction à la Cryptographie

Nadim Kobeissi

Chiffrement de Flux

- Méthode de chiffrement d’un texte, utilisant une clé.
- La taille du texte peut être arbitraire.
- Un flux de texte peut être chiffré dynamiquement au fur qu’il est produit. (exemple: conversation téléphonique)

Rappel: Chiffrement Symétrique



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

E et D sont *efficaces*, *inversibles*.

Représentation des Données

- Les operations mathématiques ne sont pas intuitifs sur les lettres. Donc, on doit representer nos messages comme des numéros.

Message	C	H	A	T	O	N
Representation ASCII	67	72	65	84	79	78
Representation Binaire	1000011	1001000	1000001	1010100	1001111	1001110

Rappel: XOR

0	0	1	1	1	0	1	0
0	1	0	1	0	0	1	1
0	1	1	0	1	0	0	1

$\oplus$

Rappel: XOR

- m est une distribution inconnue sur $\{0, 1\}^n$.
- k est une distribution **uniforme** sur $\{0, 1\}^n$.
- $c \leftarrow m \oplus k$ sera **uniforme** aussi! (Prouvé)

Le Masque Jetable ("One Time Pad")

- $c \leftarrow E(k, m) = k \oplus m$
- $m = D(k, c) = k \oplus c$

0	0	1	1	1	0	1	0
0	1	0	1	0	0	1	1
0	1	1	0	1	0	0	1

$\oplus$

Question 1

- On te donne un message m, et son chiffrement avec un masque jetable c. Est-il possible pour toi d'obtenir la clé?
  - A) Non, je ne peux pas obtenir la clé.
  - B) Oui, la clé est $k = m \oplus c$.
  - C) Oui, la clé est $k = m \oplus m$.
  - D) Je peux obtenir seulement la moitié de la clé.

Masques Jetables: Une Bonne Idée?

- ✅ Sécurité excellente.
- ✅ Performance très rapide.
- ❌ Clé aussi long que le message.
- ❌ Nom bizarre en Français.
- Le masque jetable, un chiffrement sur?

Comment Définir Un Chiffrement Sur?

- **Attaquant:** Peut attaquer le message chiffré.
- **Exigences de sécurité possibles:** L'attaquant ne peut pas…
    - Trouver la clé? $E(k,m) = m$
    - Trouver le message entier? $E(k,m_0+m_1) = m_0+E(k,m_1)$
    - Le message chiffré ne révèle <u>aucune</u> "information" sur le message clair our la clé.

Modele de Sécurité de la Théorie de l'Information

- En 1949, Claude Shannon définit ce que veut dire *"information" sur le message.*

- Un chiffrement (E, D) sur (k, m, c) est **parfaitement sur** si:

$$\forall (m_0, m_1) \qquad \text{k est uniforme } (k \xleftarrow{R} K)$$

$$\Pr[E(k,m_0)=c] = \Pr[E(k,m_1)=c]$$

Sécurité Info-Théorique: Implications

- Sachant c, on ne peut pas determiner si il correspond a m_0 ou m_1 (ou autres messages dans l'espace M).

- Même l'adversaire le plus capable n'apprend rien sur m a travers c.

Question 2

- On a un message `m`, et son chiffrement avec un masque jetable `c`. Quel est le nombre de clés possible?
  - A) Ca depend sur `m`.
  - B) 1.
  - C) 2.
  - D) Possibilités infinies.

Sécurité Info-Théorique: Implications

- Lemme: Le masque jetable est *parfaitement sur.*
- Preuve:

$$\forall (m,c)$$

$$\Pr[E(k,m)=c] = \frac{\text{Nombre de clés } k \text{ ou } E(k,m)=c}{\text{Taille de } K\ (|K|)}$$

$$= \frac{1}{\text{Taille de } K\ (|K|)}$$

La Mauvaise Nouvelle…

- Sécurité Parfaite $\longrightarrow$ $|K| \geq |M|$
- Clé aussi longue que le message.
- Comment peut-on faire un masque jetable pratique?

Chiffrement de Flux = Masque Jetable Pratique

- Remplaçons la clé “aléatoire” par une clé “pseudo-aléatoire”.

- Il suffit qu’on invente une fonction qui prend une petite clé de taille déterminée et pratique…

- et qui produit un flux **de taille arbitraire** de clés **uniques** (comme nécessité par le masque jetable!)

Rappel: Fonctions Aléatoires

- $X\colon U \longrightarrow V$
- Exemple: $X\colon \{0,1\}^n \longrightarrow \{0,1\}$
- Pour la distribution uniforme sur U:
- $Pr[X=0] = 1/2$, $Pr[X=1] = 1/2$

Chiffrement de Flux = Masque Jetable Pratique

- Remplaçons la clé “aléatoire” par une clé “pseudo-aléatoire”.

- `G` est notre fonction *déterministe* qui prend une petite “clé” et génère un flux pseudo-aléatoire interminable…

$$G: \{0,1\}^s \longrightarrow \{0,1\}^n$$

$$c \leftarrow E(k, m) = m \oplus G(k)$$

$$m = D(k, c) = c \oplus G(k)$$

Question 3

- Peut un chiffrement de flux être parfaitement sur?
  - A) Oui, si G est conçu d'une manière sure.
  - B) Non, la sécurité parfaite n'existe pas.
  - C) Oui, chaque chiffrement a une fonction qui est parfaitement sure.
  - D) Non, parce-que la clé est plus courte que le message.

Chiffrement de Flux = Masque Jetable Pratique

- Les fonctions pseudo-aléatoires ne peuvent pas adherer à la definition du chiffrement parfaitement sur.
- La sécurité de notre chiffrement de flux depend complètement sur celle de son `G`.
- Donc, il nous faut *une nouvelle definition de sécurité*.

G Doit Être Imprévisible

$G: \{0,1\}^s \longrightarrow$

0100101010010011001010100101001011010

Si l'adversaire connait une partie de l'output…

Il ne peut pas prédire ce qui vient après (ou avant, etc.)

G est prévisible si on a une fonction A tel que:

$$\Pr[A(G(k)_i) = G(k)_{i+1}] > 0.5 + \varepsilon$$

Comment Définir ε?

- **En théorie:** ε est une fonction $\varepsilon\colon Z^{\geq 0} \longrightarrow R^{\geq 0}$
- **En pratique:** ε est un numero.
  - Non-negligible: $\varepsilon \geq 1/2^{30}$ *(peut se manifester sur 1GB+)*
  - Negligible: $\varepsilon \geq 1/2^{80}$

Un Générateur Pseudo-Aléatoires Simple (non-sur)

- Générateur linéaire congruent avec paramètres `a, b, p`

```
r[i] ← a • r[i - 1] + b mod p
```

Quelle est la clé utilisée pour `G`?

`r[0]`

Pause de dix minutes.

- Après la pause:
    - Comment casser un masque jetable.
    - Exemples de systèmes de chiffrement de flux.
    - Comment casser des chiffrements de flux.
    - La sécurité sémantique.

Comment Casser un Masque Jetable

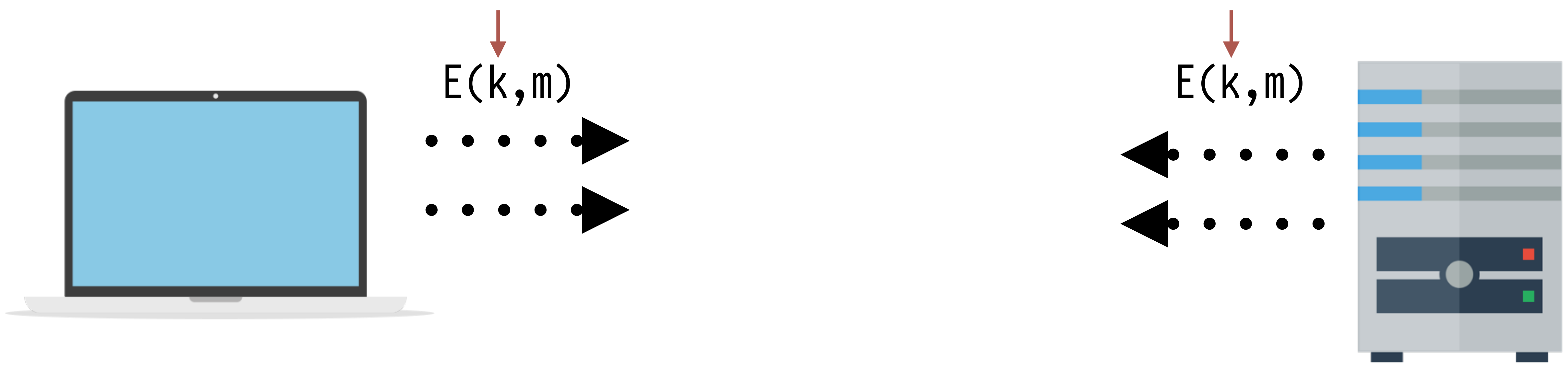
- $c_1 \leftarrow E(k, m_1) = G(k) \oplus m_1$
- $c_2 \leftarrow E(k, m_2) = G(k) \oplus m_2$

$$c_1 \oplus c_2 \quad = \quad m_1 \oplus m_2$$

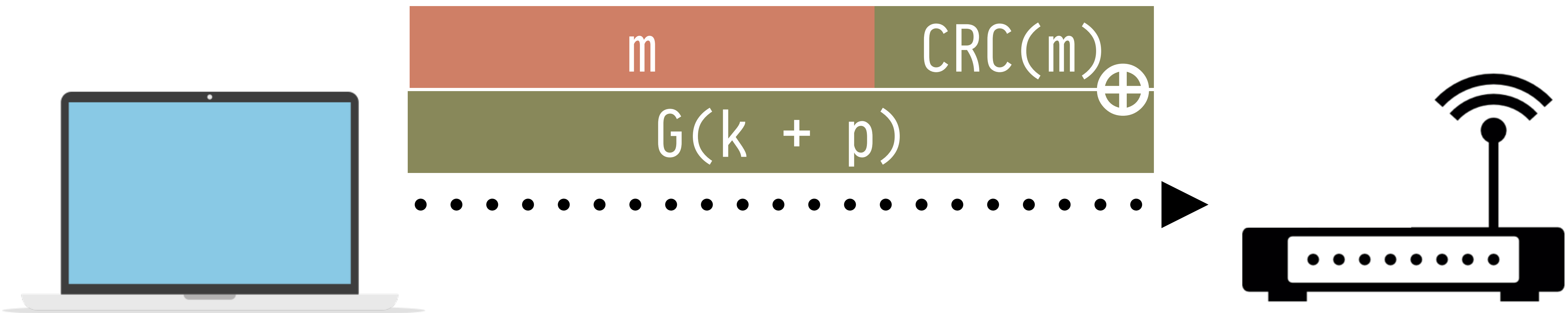
$$m_1 \oplus m_2 + \text{analyse linguistique} = m_1, m_2$$

Exemples

- Exemple: “Project Venona” (1941-1946).
- MS-PPTP (Windows NT):

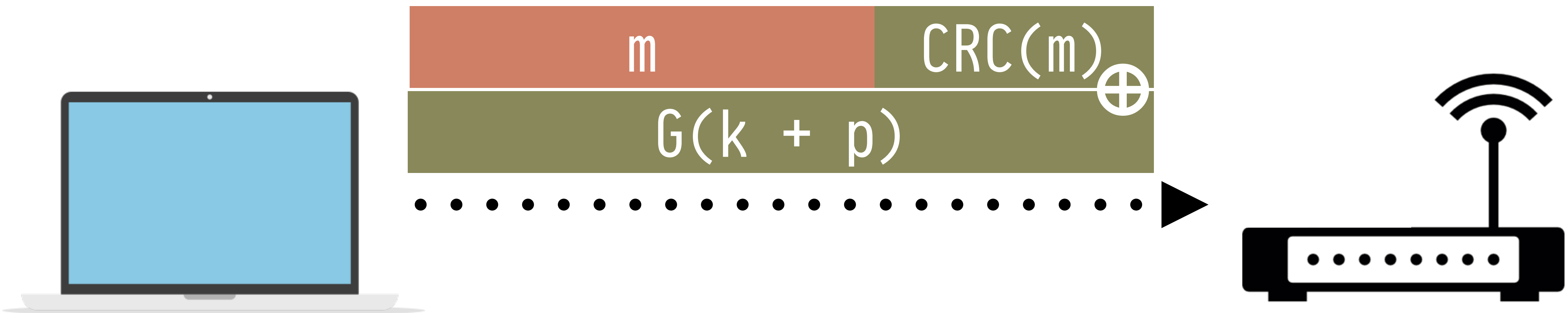


WEP: Un Exemple



- p: compteur qui incrément par 1 avec chaque paquet, pour que la clé soit différente chaque chiffrement.
    - Taille de p: 24 bits. (2^{24} = 16 millions possibilités)
    - p redevient 0 après chaque reboot sur beaucoup d'ordinateurs.

WEP: Clés Connexes



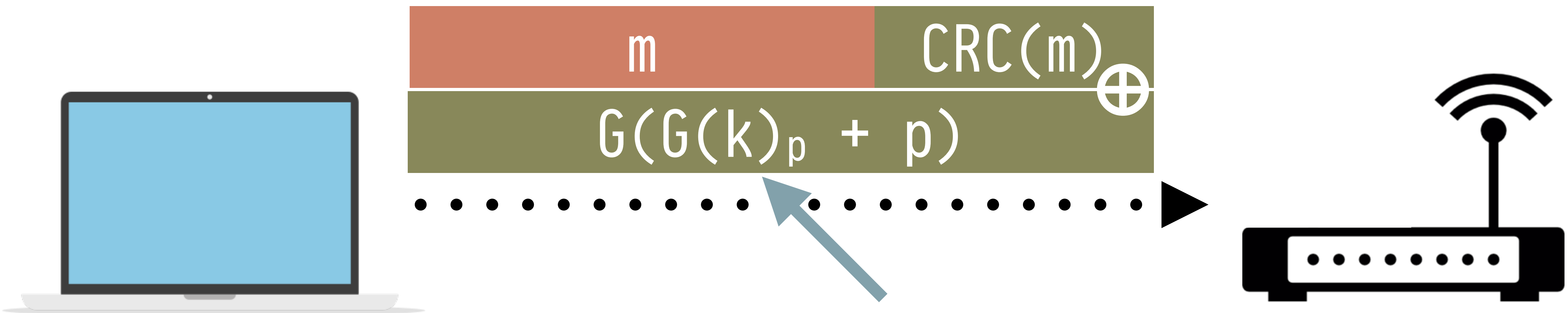
- Des failles dans le `G` utilisé (RC4) exploitent la connexion claire entre toutes les clés utilisées et casse WEP après seulement 40,000 paquets.
    - Clé pour paquet 1: `(k + 1)`
    - Clé pour paquet 2: `(k + 2)`

`k (104 bits constants)` `p`

`01001101` `01`

`128 bits en total`

Comment Améliorer WEP?



- Ginception: On utilise la sequence d'un G préliminaire comme une distributions de k différents pour un le G original.
- Meilleure idée: utilisez WPA2.

Chiffrements de Flux: Pas d'Intégrité

De: Bob

E(k, m)

De: Bob

7 25 7 $\oplus$

De: Eve

D(k, m)

De: Eve

Bob Eve

66 111 98 $\oplus$ 69 108 111

7 25 7

Question 4

- Peut-on prouver la sécurité d'un chiffrement de flux?
  - A) Oui, si `G` est conçu d'une manière sure.
  - B) Non, on ne peux pas prouver q'un `G` a un output parfaitement et infiniment aléatoire.
  - C) Dans certains cas.

Estimations heuristiques seulement

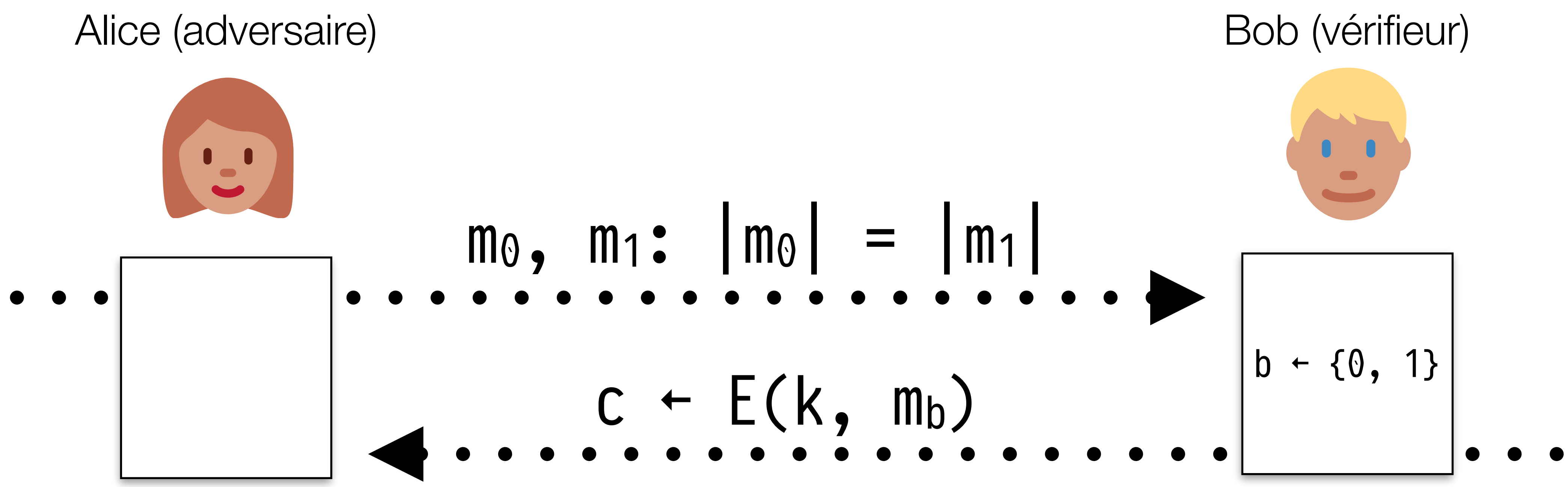
La Notion de la Sécurité Sémantique

- Shannon: un chiffrement sur ne révèle “aucune information” sur le message.

- Notre but: Obtenir plus de confiance q’un $\mathtt{G}$ “sur” = un chiffrement de flux sur.

Sécurité Sémantique

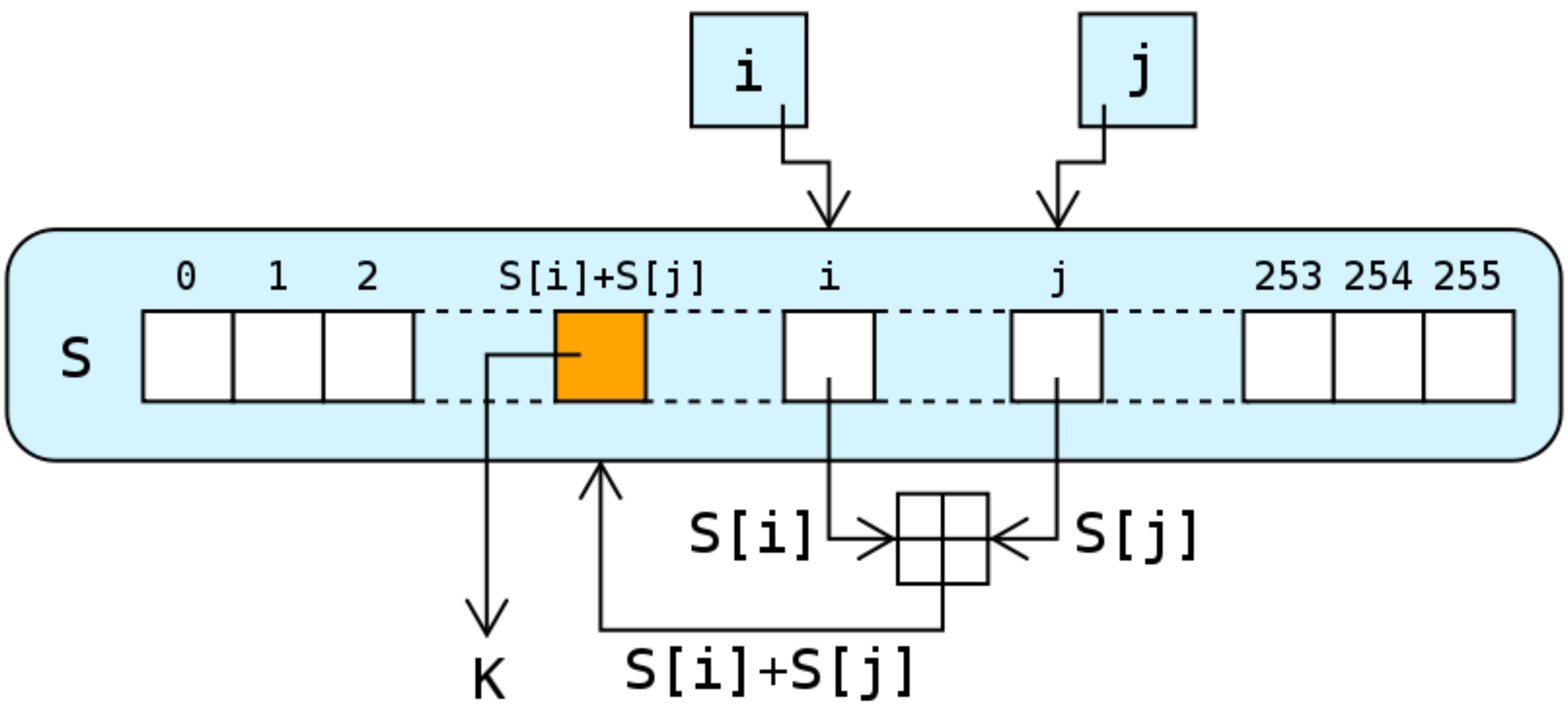
On définit deux experiments `Exp(0)` et `Exp(1)`, tel que:



`E` est *sémantiquement sur* si Alice a un avantage *negligible* avec lequel deviner la valeur de `b` en utilisant `c`.

Exemples de Chiffrements de Flux

- RC4: Cassé.
- Salsa20: Sur (utilisé par Cryptocat, miniLock…)



Suivez le Cours En Ligne

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

Grands remerciements:
- Le Loop.
- Le Jardin d'Alice.
- La Quadrature du Net.