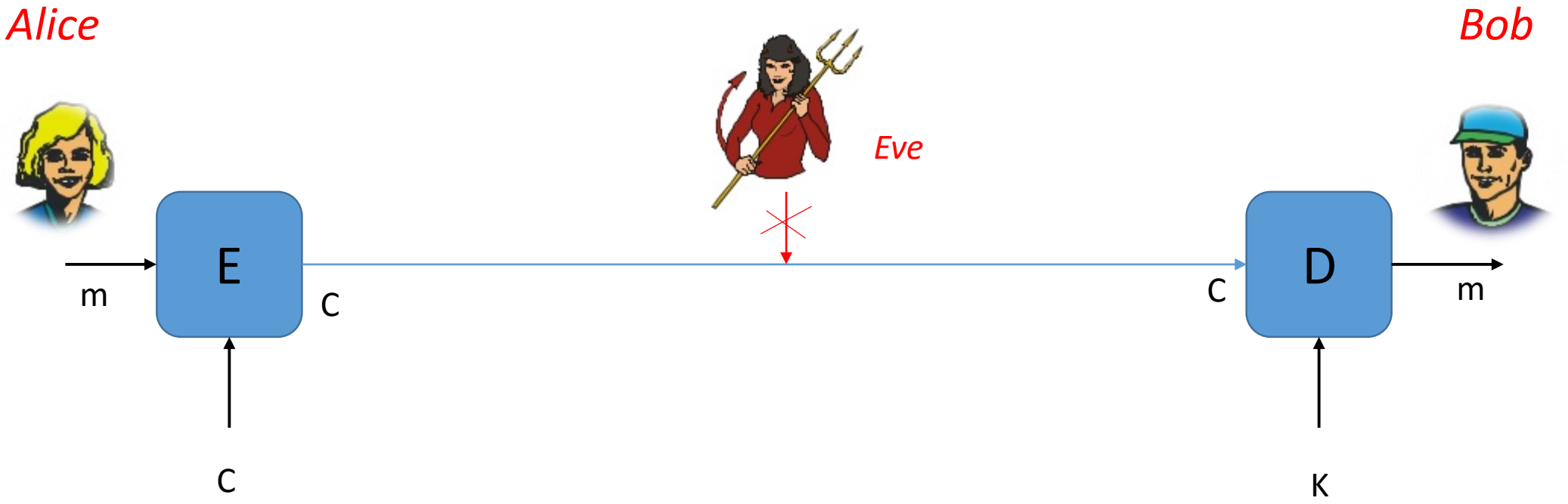
Introduction à la cryptographie 2: Chiffrement par flot

Université Paris 13 Villetaneuse

Par Houda FERRADI

Rappel : chiffrement symétrique ou à clé secrète



E (Fonction de chiffrement) et D (Fonction de déchiffrement): Fonctions inversibles et efficaces
K: Clé secrète ou symétrique
C: Le message chiffré

Chiffrement par flot

- Le **chiffrement par flot** (*stream cipher*) est une des deux grandes catégories de chiffrements modernes (*Chiffrements par flux* et *chiffrement pas bloc*), utilisant une seule clé.

- Son grand avantage : La taille de texte peut être arbitraire

- Il utilise le chiffrement symétrique: systèmes rapides et utilise des clés relativement courtes (128 à ou 256 bits)

- Il est très utilisé dans le contexte de chiffrement des communications téléphoniques (RC4, A5/1…)

Outils de base pour comprendre la crypto symétrique

- La notion du XOR (ou le « ou » exclusif)
- Savoir représenter des données en binaires
- Comprendre la probabilité discrète
- Connaitre la notion de l'entropie de Shannon
- Simuler des générateurs pseudo aléatoires

Rappel : Probabilité discrète

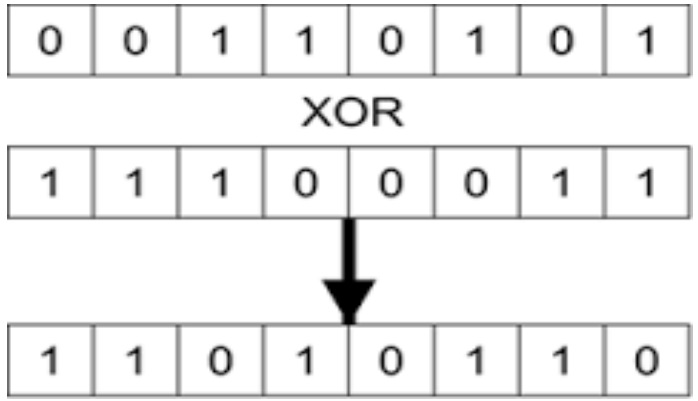
- Une distribution de probabilité suit une loi uniforme lorsque toutes les valeurs prises par la *variable aléatoire* sont *équiprobables*. Si n est le nombre de valeurs différentes prises par la variable aléatoire:

- $\forall\, i, P(X = x\_i) = \frac{1}{n}$
- Exemple: Si U est un ensemble fini et $U = \{0,1\}^n$
- Etant U=$\{0,I\}^2$, U a une distribution uniforme 

Pour chaque $\{00\}$,$\{0I\}$,$\{II\}$,$\{I0\}$, la probabilité est: $P(X) = 0{,}25$ tel que $\sum P(X) = 1$

Rappel sur le XOR

L'application de l'opération XOR étant simple en informatique, ces traitements peuvent s'effectuer à très grande vitesse.



Propriétés mathématique du XOR:

$A \oplus B = \overline{A}B + \overline{B}A$

$A \oplus \overline{A} = 1$

$A \oplus 0 = A$

$A \oplus 1 = \overline{A}$

$A \oplus B = B \oplus A$

$(A \oplus B) \oplus B = A$

Si $A \oplus B = C$ alors $C \oplus B = A$ et $A \oplus C = B$

Rappel sur les propriétés d'un XOR

La probabilité discrète uniforme est assurée par la propriété du XOR:

Etant:

- Y est une distribution inconnue sur $\{0,1\}^n$
- X est une distribution uniforme sur $\{0,1\}^n$

Alors: Z:= Y$\oplus$X sera uniforme aussi!

Masque jetable ou le OTP « One Time Pad »

- Le masque jetable utilise la propriété du XOR qui permet d'obtenir une *probabilité discrète uniforme.*

- Masque jetable inventé par *Vernam* en 1917 et amélioré par *Mauborne* qui a introduit la notion de *la clé aléatoire.*

- Système théoriquement « incassable » et *parfaitement sûr* mais dans la pratique *impossible* d'être implémenté correctement ! (explication dans ce cours)

Comment marche un Masque Jetable ?

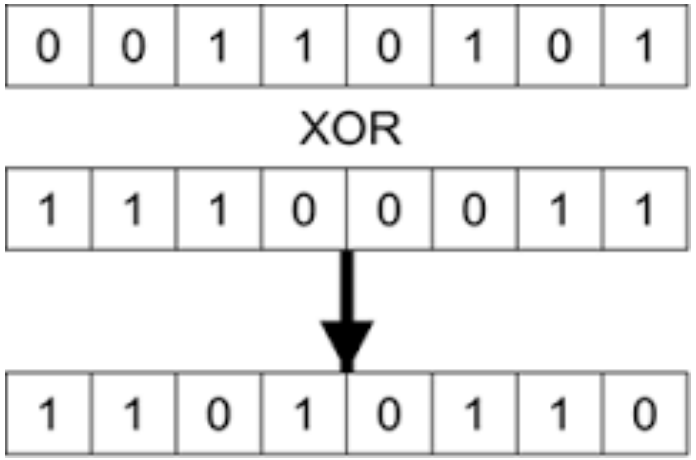
Principe d'un masque jetable :

- Clé doit être utilisé *une seule* fois (d'où le terme jetable)
- La taille de la clé doit être *aussi longue* que le message
- Les bits composant la clé, ou « masque » doivent être choisis *aléatoirement*

Le Masque Jetable ou le « One Time Pad »

Le chiffrement est donné par l'utilisation d'un OU Exclusif « XOR » entre le message à chiffrer et la clé modulo 2:

- La méthode du chiffrement: $c \leftarrow E(k,m) = k \oplus m$
- La méthode du déchiffrement: $m \leftarrow D(k,c) = k \oplus c$



Masque Jetable

Le masque jetable a de très bonnes avantages:

- *Sécurité inconditionnelle:* Probabilité discrète *uniforme* des messages chiffrés
- *Efficacité:* XOR est très simple à calculer en informatique

Inconvénients:

- *Clé aussi longue que le message:* Problème de Stockage, d'accessibilité et de confidentialité des clés.

Rappel : Sécurité Inconditionnelle (ou Parfaite)

- Claude Shannon en 1949 dans son article « Communication theory of secrecy systems », a introduit la notion de l'« information » sur un message et de l'entropie.

Rappel : Sécurité Inconditionnelle (ou Parfaite)

Plus formellement: *Si on choisit une clé différente pour chaque message* alors *un système cryptographique est parfaitement sûr* ssi :

$$\forall \mathrm{x} \in M, \forall \mathrm{y} \in C, P(x|y) = P(x)$$

Autrement dit: la probabilité d'un texte clair x sachant que le texte chiffré est y est la même que la probabilité de n'importe quel x. Le texte chiffré dans ce cas n'apporte aucune information sur le texte clair.

Exemple d'une sécurité inconditionnelle(ou parfaite)

- Si on tire *aléatoirement* une clé k d'un espace de clé K: $k \xleftarrow{R} K$

- Etant une fonction de chiffrement E et de déchiffrement D. Une clé k , un message m et un chiffre c: (k, m, c)

Un chiffrement E est sûr si:

$$\forall (m_0, m_1)$$

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

Autrement dit: La probabilité d'un texte clair m_0 sachant que le texte chiffré est C est la même que la probabilité de m_1. Le texte chiffré dans ce cas n'apporte *aucune information* sur le texte clair.

Implications Théoriques

Lemme: Le masque jetable est *parfaitement sûr*

Preuve: $\forall\ (m, c)$

$$P(E(k,m) = c) = \frac{Nombre\ de\ clés\ utilisés\ par\ chiffré\ c}{Taille\ de\ l'espace\ de\ clés\ K}$$

- Sachant que le masque jetable utilise **I** clé par chiffré "**c**".
- Alors on obtient : $\frac{1}{Taille\ de\ clés\ K}$, qui représente une *probabilité maximale* pour une *sécurité parfaite.*

Implications Théoriques du « OTP »

1. Un attaquant à partir d'un chiffré c, il ne peut pas distingué que c'est un chiffré de de m_0 ou de m_1

2. Même si on suppose l'adversaire le plus « puissant », il n'apprendrait aucune information sur le message m à partir de son chiffré c.

3. Le masque jetable remplit la condition $|K| = |M|$ qui signifie que *les clés sont équiprobables : Pour* $\forall x \in M \quad et \quad \forall y \in C$, il existe une unique clé verifiant $f(x) = y$ *(tel que la fonction* $f()$ *est bijective)*

Implication Pratique du « OTP »

- Pour une *sécurité parfaite*, il faut obtenir : $|K| = |M|$ (condition impossible à obtenir aujourd'hui avec les générateurs de nombres aléatoires actuels)

- Faut que les clés soient aussi *longues* que le message, et donc un espace de stockage très grand.

Question: Comment optimiser la sécurité d'un masque jetable en pratique ?