Cryptographie
Bases et One Time Pad

Carlos Aguilar

carlos.aguilar@enseeiht.fr

IRIT-IRT

Références

Livres électroniques

Cornell, https://www.cs.cornell.edu/courses/cs4830/2010fa/lecnotes.pdf
Bristol, http://www.cs.umd.edu/~waa/414-F11/IntroToCrypto.pdf
Stanford, http://crypto.stanford.edu/~dabo/cryptobook/

Cours fortement inspiré de :

[1] Stanford, https://www.coursera.org/course/crypto
[2] Univ. of Virginia, http://www.udacity.com/view#Course/cs387/

Plan

Qu'est ce que la cryptographie ?

C'est ...

- Un outil indispensable
- La base de nombreux protocoles de sécurité

C'est pas ...

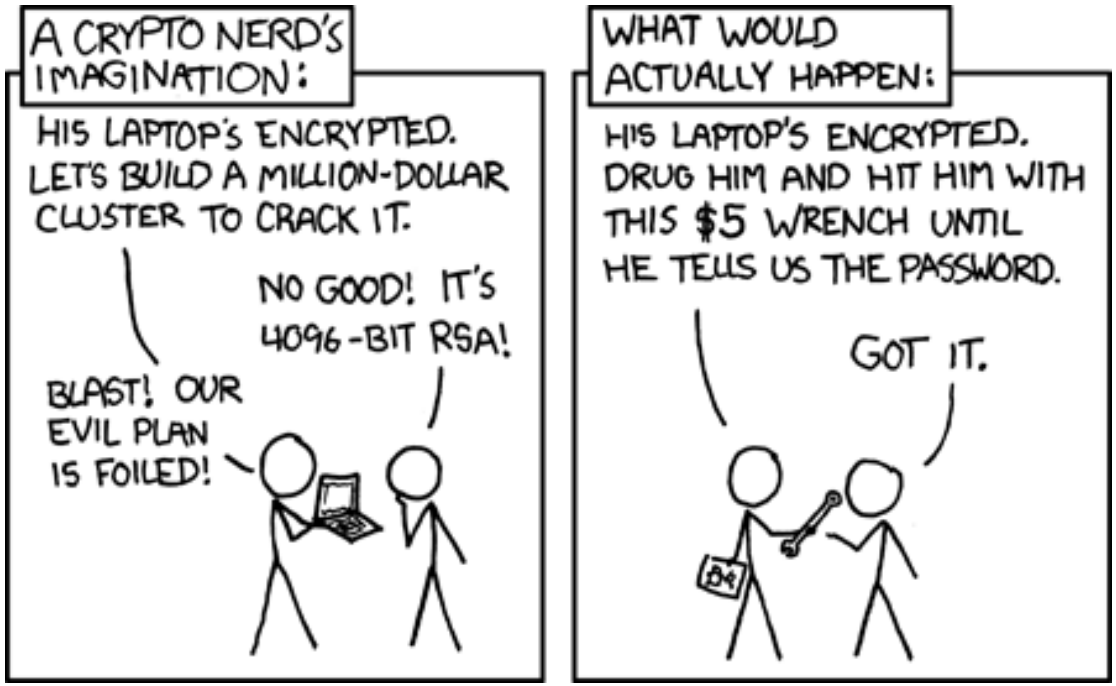
- La solution à tout problème
- Sûr sauf si implémenté correctement
- Sûr sauf si utilisé correctement

Et surtout ...

C'est pas forcément incompréhensible ! (ça peut même être rigolo, sisi)

Qu'est ce que la cryptographie ?

http://www.xkcd.com



Un petit quiz [2]

Définitions

Cryptographie : “L’écriture des secrets”
Cryptologie : “La science du secret”

Lesquelles de ces actions ont un rapport avec la cryptologie ?

1. Ouvrir une porte
2. Jouer au poker
3. Se connecter à un compte (sur le net)
4. Faire une recherche avec Google

Connectez vous avec `nc prof-301.local 31000` et tapez la réponse (e.g. 1 ou 12 ou 234 ou 123 ou 1234 ou 0 si tout est faux) puis entrée

Un petit quiz [2]

Définitions

Cryptographie : “L’écriture des secrets”
Cryptologie : “La science du secret”

Lesquelles de ces actions ont un rapport avec la cryptologie ?

1. Ouvrir une porte
2. Jouer au poker
3. Se connecter à un compte (sur le net)
4. Faire une recherche avec Google

Connectez vous avec `nc prof-301.local 31000` et tapez la réponse (e.g. 1 ou 12 ou 234 ou 123 ou 1234 ou 0 si tout est faux) puis entrée

Tirages

Ensembles et distributions

Une distribution χ sur un ensemble S est (en simplifiant) une fonction qui associe à chaque élément de S une probabilité

Tirages

On note $x \xleftarrow{\chi} S$ ou $x \leftarrow (S, \chi)$ la définition de x comme le tirage d'un élément de S en suivant la distribution de probabilités χ

On simplifie en notant $x \leftarrow S$:

- quand on tire un élément uniformément au hasard de S
- quand S est sans équivoque lié à une distribution

La loi uniforme, s'il faut l'indiquer explicitement, sera notée U

Fonctions et algorithmes

Notation fonctionnelle

Pour une fonction il y a une unique sortie possible on note $f(x) = y$ car y est l'unique résultat possible quand on applique la fonction f à l'entrée x

Pour les algorithmes il y a deux cas très différents : les algorithmes déterministes et les algorithmes randomisés

Algorithmes déterministes

Pour une entrée il y a une unique sortie possible
$\Rightarrow$ on utilise une notation fonctionnelle $A(x) = y$

Algorithmes randomisés

Pour une entrée (x) il y a un ensemble de résultats possibles (S, appelé ensemble des sorties) et une distribution (χ, appelée distribution de sortie) associant à chaque résultat une probabilité : $A(x) = (S, \chi)$

Sorties d'un algorithme

Algorithmes et ensemble des sorties possibles

Souvent on ignore la distribution et on considère $A(x)$ comme un ensemble

Ainsi $y \in A(x)$ veut dire $y \in S$ pour $A(x) = (S, \chi)$ (i.e. que y est une des sorties possibles de l'algorithme randomisé A quand il prend x en entrée)

Algorithmes et tirages

Quand on définit y comme la sortie d'une exécution d'un algorithme randomisé A pour une entrée x on note tout simplement $y \leftarrow A(x)$

Définir y par une exécution correspond bien à un tirage parmi l'ensemble de sorties de $A(x)$ en suivant la distribution de sortie

Composition

Avec des fonctions : $g(f(x))$ "appliquer f à x et appliquer g au résultat"
Avec les algorithmes randomisés que veut dire $B(A(x))$?

Plan

Définitions du chiffrement

Termes français

- Clair : message non chiffré $m \in \mathcal{M}$
- Chiffré : message chiffré $c \in \mathcal{C}$
- Clé symétrique : secret permettant de chiffrer/déchiffrer $sk \in \mathcal{K}$
- Chiffrement : passage d'un clair à un chiffré $c \leftarrow Enc(sk, m)$
- Déchiffrement : passage d'un chiffré à un clair $m \leftarrow Dec(sk, c)$
- Canal sûr : pour échanger les clés
- Canal non sûr : pour envoyer/stocker les données
- Crypter/Décrypter : a proscrire
- Clé secrète : ambigu

Termes anglais

Plaintext, ciphertext, symetric key, encryption, decryption, secure channel, insecure channel, N/A, secret key (ambiguous)

Le chiffrement

Utilité et limites

Permet de cacher des informations (échangées ou stockées).

- N'occulte pas la présence/taille/timing des données
- N'évite pas les modifications/rejeus
- On ne peut pas tout chiffrer (par ex. infos de routage)

Principe de Kerckhoff (1883) sur le secret des algorithmes

"Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi"

Ne réside pas dans l'algorithme utilisé mais dans une de ses entrées : la clé

Algos symétriques : une seule clé (secrète) pour chiffrer et déchiffrer
Algos asymétriques : clé publique pour chiffrer, secrète pour déchiffrer

Un autre principe : la (bi-)clé doit être petite !

Symétrique vous dites ?

Une même clé pour chiffrer et déchiffrer

Alice veut envoyer un message à Bob

- Alice chiffre le clair en utilisant une clé sk et obtient un chiffré
- Alice envoie le chiffré ou le met dans un endroit où Bob peut le récupérer (par ex. sur le frigo)
- Bob utilise **la même clé** sk pour déchiffrer le message reçu

Plus formellement

- Chiffrement d'un clair m : $c \leftarrow Enc(sk, m)$
- Déchiffrement d'un chiffré c : $m \leftarrow Dec(sk, c)$
- Consistance : $\forall m, sk : Dec(sk, Enc(sk, m)) = \{m\}$
- Sécurité : les chiffrés ne dévoilent rien sur les messages ou la clé

Un autre quiz [2]

Lequel de ces chiffrements symétriques est consistant ?

$\mathcal{M} = \mathcal{C} = \mathcal{K} = \{1, 2, 3, \ldots\}$

1. $Enc(k, m) = k + m$, $Dec(k, c) = c - k$
2. $Enc(k, m) = m$, $Dec(k, c) = c$
3. $Enc(k, m) = m\%k$, $Dec(k, c) = c * k$

Un autre quiz [2]

Lequel de ces chiffrements symétriques est consistant ?

$\mathcal{M} = \mathcal{C} = \mathcal{K} = \{1, 2, 3, \ldots\}$

1. $Enc(k, m) = k + m$, $Dec(k, c) = c - k$
2. $Enc(k, m) = m$, $Dec(k, c) = c$
3. $Enc(k, m) = m\%k$, $Dec(k, c) = c * k$

Plan

XOR à la rescousse

Notation

$\oplus$ = XOR = “OU-exclusif” = “Somme modulo 2” :
$0 \oplus 0 = 1 \oplus 1 = 0$, $0 \oplus 1 = 1 \oplus 0 = 1$

Quiz [2] : Que vaut $x \oplus y \oplus x$?

1. 0
2. x
3. y
4. Ça dépend de x

Comment l’appliquer à la cryptographie ?

XOR à la rescousse

Notation

$\oplus$ = XOR = “OU-exclusif” = “Somme modulo 2” :
$0 \oplus 0 = 1 \oplus 1 = 0$, $0 \oplus 1 = 1 \oplus 0 = 1$

Quiz [2] : Que vaut $x \oplus y \oplus x$?

1. 0
2. x
3. y
4. Ça dépend de x

Comment l’appliquer à la cryptographie ?

Un chiffrement symétrique parfaitement sûr et simple

Le One Time Pad (Vernam, 1917)

message $\oplus$ clé = chiffré chiffré $\oplus$ clé = message

```
message : 0 1 0 1 1 1 1 0 0 0 0 1 0 0 1
clé     : 1 1 0 0 0 1 0 1 0 0 0 1 1 1 0
=======================================
chiffré : 1 0 0 1 1 0 1 1 0 0 0 1 1 1 1
```

Sécurité (première tentative)

La distribution en sortie est uniforme

$$\begin{aligned} P(c_i = 1) &= P(k_i = 1 \cap m_i = 0) + P(k_i = 0 \cap m_i = 1) \\ &= P(k_i = 1) * P(m_i = 0) + P(k_i = 0) * P(m_i = 1) \\ P(c_i = 1) &= 1/2 \end{aligned}$$

Un chiffrement symétrique parfaitement sûr et simple

Le One Time Pad (Vernam, 1917)

message $\oplus$ clé = chiffré chiffré $\oplus$ clé = message

```
message : 0 1 0 1 1 1 1 0 0 0 0 1 0 0 1
clé     : 1 1 0 0 0 1 0 1 0 0 0 1 1 1 0
=======================================
chiffré : 1 0 0 1 1 0 1 1 0 0 0 1 1 1 1
```

Sécurité (seconde tentative)

Pour un chiffré tout clair est possible

Un chiffrement symétrique parfaitement sûr et simple

Le One Time Pad (Vernam, 1917)

message $\oplus$ clé = chiffré chiffré $\oplus$ clé = message

```
message : 0 1
clé     : 1 1
=======================================
chiffré : 1 0
```

Sécurité (seconde tentative)

Pour un chiffré tout clair est possible

Un chiffrement symétrique parfaitement sûr et simple

Le One Time Pad (Vernam, 1917)

message $\oplus$ clé = chiffré chiffré $\oplus$ clé = message

```
message : X X
clé     : X X
=======================================
chiffré : 1 0
```

Sécurité (seconde tentative)

Pour un chiffré tout clair est possible

Un chiffrement symétrique parfaitement sûr et simple

Le One Time Pad (Vernam, 1917)

message $\oplus$ clé = chiffré chiffré $\oplus$ clé = message

```
message : X X       0 0 | 0 1 | 1 0 | 1 1
clé     : X X       1 0 | 1 1 | 0 0 | 0 1
=================================================
chiffré : 1 0       1 0 | 1 0 | 1 0 | 1 0
```

Sécurité (seconde tentative)

Pour un chiffré tout clair est possible

Un chiffrement symétrique parfaitement sûr et simple

L'OTP est-il parfaitement sûr ?

Quiz [2] : Quelle propriété on peut souhaiter ?

Y chiffré vu par l'attaquant, X clair associé

1. $\forall m, c : P[X = m | Y = c] = 1/|M|$
2. $\forall m, c : P[X = m | Y = c] = P[X = m]$
3. $\forall m, c : P[X = m] = P[Y = c]$
4. $\forall m, c : P[X = m | Y = c] = 1/|K|$

Un chiffrement symétrique parfaitement sûr et simple

L'OTP est-il parfaitement sûr ?

Quiz [2] : Quelle propriété on peut souhaiter ?

Y chiffré vu par l'attaquant, X clair associé

1. $\forall m, c : P[X = m | Y = c] = 1/|M|$
2. $\forall m, c : P[X = m | Y = c] = P[X = m]$
3. $\forall m, c : P[X = m] = P[Y = c]$
4. $\forall m, c : P[X = m | Y = c] = 1/|K|$

Un chiffrement symétrique parfaitement sûr et simple

L'OTP est-il parfaitement sûr ?

$P[A|B] = P[A \cap B]/P[B]$
A, B indépendants $\Leftrightarrow P[A \cap B] = P[A] * P[B] \Leftrightarrow P[A|B] = P[A]$
$P[B] = \sum P[A_i \cap B]$ pour A_i un partitionnement de Ω

Quiz [2] : Quelle propriété on peut souhaiter ?

Y chiffré vu par l'attaquant, X clair associé

1. $\forall m, c : P[X = m|Y = c] = 1/|M|$
2. $\forall m, c : P[X = m|Y = c] = P[X = m]$
3. $\forall m, c : P[X = m] = P[Y = c]$
4. $\forall m, c : P[X = m|Y = c] = 1/|K|$

Un chiffrement symétrique parfaitement sûr et simple

L'OTP est-il parfaitement sûr ?

$P[A|B] = P[A \cap B]/P[B]$
A, B indépendants $\Leftrightarrow P[A \cap B] = P[A] * P[B] \Leftrightarrow P[A|B] = P[A]$
$P[B] = \sum P[A_i \cap B]$ pour A_i un partitionnement de Ω

$P[X = m|Y = c] = P[X = m \cap Y = c]/P[Y = c]$

Quiz [2] : Quelle propriété on peut souhaiter ?

Y chiffré vu par l'attaquant, X clair associé

1. $\forall m, c : P[X = m|Y = c] = 1/|M|$
2. $\forall m, c : P[X = m|Y = c] = P[X = m]$
3. $\forall m, c : P[X = m] = P[Y = c]$
4. $\forall m, c : P[X = m|Y = c] = 1/|K|$

Un chiffrement symétrique parfaitement sûr et simple

L'OTP est-il parfaitement sûr ?

$P[A|B] = P[A \cap B]/P[B]$
A, B indépendants $\Leftrightarrow P[A \cap B] = P[A] * P[B] \Leftrightarrow P[A|B] = P[A]$
$P[B] = \sum P[A_i \cap B]$ pour A_i un partitionnement de Ω

$P[X = m|Y = c] = P[X = m \cap Y = c]/P[Y = c]$
$P[Y = c] = \sum_{i \in M} P[X = i \cap Y = c]$

Quiz [2] : Quelle propriété on peut souhaiter ?

Y chiffré vu par l'attaquant, X clair associé

1. $\forall m, c : P[X = m|Y = c] = 1/|M|$
2. $\forall m, c : P[X = m|Y = c] = P[X = m]$
3. $\forall m, c : P[X = m] = P[Y = c]$
4. $\forall m, c : P[X = m|Y = c] = 1/|K|$

Un chiffrement symétrique parfaitement sûr et simple

L'OTP est-il parfaitement sûr ?

$P[A|B] = P[A \cap B]/P[B]$
A, B indépendants $\Leftrightarrow P[A \cap B] = P[A] * P[B] \Leftrightarrow P[A|B] = P[A]$
$P[B] = \sum P[A_i \cap B]$ pour A_i un partitionnement de Ω

$P[X = m | Y = c] = P[X = m \cap Y = c]/P[Y = c]$
$P[Y = c] = \sum_{i \in M} P[X = i \cap Y = c]$

Quiz [2] : Combien de clés sont possibles pour $X = i \cap Y = c$?

Un nombre 1,2,3,4,..
Une gamme 0-1, 0-K, 1-K

Un chiffrement symétrique parfaitement sûr et simple

L'OTP est-il parfaitement sûr ?

$P[A|B] = P[A \cap B]/P[B]$
A, B indépendants $\Leftrightarrow P[A \cap B] = P[A] * P[B] \Leftrightarrow P[A|B] = P[A]$
$P[B] = \sum P[A_i \cap B]$ pour A_i un partitionnement de Ω

$P[X = m | Y = c] = P[X = m \cap Y = c]/P[Y = c]$
$P[Y = c] = \sum_{i \in M} P[X = i \cap Y = c]$

Quiz [2] : Combien de clés sont possibles pour $X = i \cap Y = c$?

Un nombre 1,2,3,4,..
Une gamme 0-1, 0-K, 1-K

Un chiffrement symétrique parfaitement sûr et simple

L'OTP est-il parfaitement sûr ?

$P[A|B] = P[A \cap B]/P[B]$
A, B indépendants $\Leftrightarrow P[A \cap B] = P[A] * P[B] \Leftrightarrow P[A|B] = P[A]$
$P[B] = \sum P[A_i \cap B]$ pour A_i un partitionnement de Ω

$P[X = m | Y = c] = P[X = m \cap Y = c]/P[Y = c]$
$P[Y = c] = \sum_{i \in M} P[X = i \cap Y = c]$
$P[Y = c] = \sum_{i \in M} P[X = i \cap K = c \oplus i]$

Quiz [2] : Combien de clés sont possibles pour $X = i \cap Y = c$?

Un nombre 1,2,3,4,..
Une gamme 0-1, 0-K, 1-K

Un chiffrement symétrique parfaitement sûr et simple

L'OTP est-il parfaitement sûr ?

$P[A|B] = P[A \cap B]/P[B]$
A, B indépendants $\Leftrightarrow P[A \cap B] = P[A] * P[B] \Leftrightarrow P[A|B] = P[A]$
$P[B] = \sum P[A_i \cap B]$ pour A_i un partitionnement de Ω

$P[X = m|Y = c] = P[X = m \cap Y = c]/P[Y = c]$
$P[Y = c] = \sum_{i \in M} P[X = i \cap Y = c]$
$P[Y = c] = \sum_{i \in M} P[X = i \cap K = c \oplus i]$

Quiz [2] : Que vaut $P[X = i \cap K = c \oplus i]$?

1. $1/|K|$
2. $1/(|M| * |K|)$
3. $P[X = i]/|K|$
4. $P[X = i]$

Un chiffrement symétrique parfaitement sûr et simple

L'OTP est-il parfaitement sûr ?

$P[A|B] = P[A \cap B]/P[B]$
A, B indépendants $\Leftrightarrow P[A \cap B] = P[A] * P[B] \Leftrightarrow P[A|B] = P[A]$
$P[B] = \sum P[A_i \cap B]$ pour A_i un partitionnement de Ω

$P[X = m | Y = c] = P[X = m \cap Y = c]/P[Y = c]$
$P[Y = c] = \sum_{i \in M} P[X = i \cap Y = c]$
$P[Y = c] = \sum_{i \in M} P[X = i \cap K = c \oplus i]$

Quiz [2] : Que vaut $P[X = i \cap K = c \oplus i]$?

1. $1/|K|$
2. $1/(|M| * |K|)$
3. $P[X = i]/|K|$
4. $P[X = i]$

Un chiffrement symétrique parfaitement sûr et simple

L'OTP est-il parfaitement sûr ?

$P[A|B] = P[A \cap B]/P[B]$
A, B indépendants $\Leftrightarrow P[A \cap B] = P[A] * P[B] \Leftrightarrow P[A|B] = P[A]$
$P[B] = \sum P[A_i \cap B]$ pour A_i un partitionnement de Ω

$P[X = m|Y = c] = P[X = m \cap Y = c]/P[Y = c]$
$P[Y = c] = \sum_{i \in M} P[X = i \cap Y = c]$
$P[Y = c] = \sum_{i \in M} P[X = i \cap K = c \oplus i] = \sum_{i \in M} P[X = i]/|K| = 1/|K|$

Quiz [2] : Que vaut $P[X = i \cap K = c \oplus i]$?

1. $1/|K|$
2. $1/(|M| * |K|)$
3. $P[X = i]/|K|$
4. $P[X = i]$

Un chiffrement symétrique parfaitement sûr et simple

L'OTP est-il parfaitement sûr ?

$P[A|B] = P[A \cap B]/P[B]$
A, B indépendants $\Leftrightarrow P[A \cap B] = P[A] * P[B] \Leftrightarrow P[A|B] = P[A]$
$P[B] = \sum P[A_i \cap B]$ pour A_i un partitionnement de Ω

$P[X = m|Y = c] = P[X = m \cap Y = c]/P[Y = c]$
$P[Y = c] = \sum_{i \in M} P[X = i \cap Y = c]$
$P[Y = c] = \sum_{i \in M} P[X = i \cap K = c \oplus i] = \sum_{i \in M} P[X = i]/|K| = 1/|K|$
$P[X = m \cap Y = c] = P[X = m \cap K = c \oplus m] = P[X = m] * 1/|K|$

Quiz [2] : Que vaut $P[X = i \cap K = c \oplus i]$?

1. $1/|K|$
2. $1/(|M| * |K|)$
3. $P[X = i]/|K|$
4. $P[X = i]$

Parfaitement sûr et simple ... mais peu pratique

Problèmes de Malléabilité

Si un attaquant voit passer un chiffré c du clair m et il le modifie en $c' = c \oplus x$ alors c' aura pour clair associé $m' = m \oplus x$

Problèmes de gestion de clé

Clé aussi grande que le message et non réutilisable ! !
$c_1 \oplus c_2 = (m_1 \oplus k) \oplus (m_2 \oplus k) = m_1 \oplus m_2$

Les mauvaises nouvelles

Théorème de Shanon

Si un système de chiffrement est parfaitement sûr, alors $|K| \geq |M|$

Preuve

Supposons par l'absurde que $|K| < |M|$ et qu'un attaquant étudie $Y = c$
Si il calcule $M_0 = \cup_{k \in K} Dec(k, c)$ on aura $|M_0| < |M|$
$\Rightarrow$ pour $m \notin M_0$, $P[X = m \mid Y = c] = 0$ même si $P[X = m] = 1/|M|$

L'uniformité écrase la singularité

Retour sur la première propriété de sécurité

$\forall i : P(c_i = 1) = 1/2$ quelle que soit la distribution des messages !
$X, Y, Z = X \oplus Y$ sur un même espace, si Y uniforme et X indép. Z uniforme

Variantes

X c'est Mme. Non, X c'est Mme. Oui, X uniforme, X c'est M. Bavard, ...
Mais aussi si $X = X_1 \oplus X_2$, $X = C_1 \oplus X_1 \oplus C_2$, ...

Dans tous les cas si Y indépendant de X et uniforme $X \oplus Y$ uniforme

Négociation d'aléa

A et B veulent négocier une valeur commune uniformément aléatoire, mais ils sont méfiants l'un de l'autre (qui peut pervertir le choix)

Comment faire ?

L'uniformité écrase la singularité

Retour sur la première propriété de sécurité

$\forall i : P(c_i = 1) = 1/2$ quelle que soit la distribution des messages !
$X, Y, Z = X \oplus Y$ sur un même espace, si Y uniforme et X indép. Z uniforme

Variantes

X c'est Mme. Non, X c'est Mme. Oui, X uniforme, X c'est M. Bavard, ...
Mais aussi si $X = X_1 \oplus X_2$, $X = C_1 \oplus X_1 \oplus C_2$, ...

Dans tous les cas si Y indépendant de X et uniforme $X \oplus Y$ uniforme

Négociation d'aléa

A et B veulent négocier une valeur commune uniformément aléatoire, mais ils sont méfiants l'un de l'autre (qui peut pervertir le choix)

Comment faire ?
$A : x \xleftarrow{\chi} \Omega$, $B : y \xleftarrow{\chi'} \Omega$, $v = x \oplus y$, si $\chi = U$ ou $\chi' = U$, v est uniform. distrib.
Attention ! Il faut que les envois soient simultanés (solution : suite du cours)

Probabilités Conditionnelles [2]

Fréquence voyelles en français

e 15%, a 8%, i 8%, u 6%, o 5%

Que vaut P[X est une voyelle] ?

Que vaut $P[X = \text{'e'}|\text{X est une voyelle}]$?

Que vaut $P[\text{X est une voyelle}|X \neq \text{'a'}]$?

Probabilités Conditionnelles [2]

Fréquence voyelles en français

e 15%, a 8%, i 8%, u 6%, o 5%

Que vaut P[X est une voyelle] ?

P[X est une voyelle] $= 0.15 + 0.08 + 0.08 + 0.06 + 0.05 = 0.42$

Que vaut $P[X = \text{'e'} | \text{X est une voyelle}]$?

Que vaut $P[\text{X est une voyelle} | X \neq \text{'a'}]$?

Probabilités Conditionnelles [2]

Fréquence voyelles en français

e 15%, a 8%, i 8%, u 6%, o 5%

Que vaut P[X est une voyelle] ?

P[X est une voyelle] $= 0.15 + 0.08 + 0.08 + 0.06 + 0.05 = 0.42$

Que vaut $P[X = \text{'e'}|\text{X est une voyelle}]$?

$P[X = \text{'e'}|\text{X est une voyelle}] =$
$P[X = \text{'e'} \cap \text{X est une voyelle}]/P[\text{X est une voyelle}] = 0.15/0.42 = 0.36$

Que vaut $P[\text{X est une voyelle}|X \neq \text{'a'}]$?

Probabilités Conditionnelles [2]

Fréquence voyelles en français

e 15%, a 8%, i 8%, u 6%, o 5%

Que vaut P[X est une voyelle] ?

P[X est une voyelle] $= 0.15 + 0.08 + 0.08 + 0.06 + 0.05 = 0.42$

Que vaut $P[X =$ 'e'$|$X est une voyelle$]$?

$P[X =$ 'e'$|$X est une voyelle$] =$
$P[X =$ 'e' $\cap$ X est une voyelle$]/P$[X est une voyelle$] = 0.15/0.42 = 0.36$

Que vaut P[X est une voyelle$|X \neq$ 'a'$]$?

P[X est une voyelle$|X \neq$ 'a'$] =$
$P[X \in \{$'e','i','o','u'$\}]/P[X \neq$ 'a'$] = 0.34/0.92 = 0.37$

OTP : Malléabilité [2]

Contexte

Alice et Bob sont d'accord sur une clé, ils veulent s'échanger un message "O"ou "N" (pour oui et non) en utilisant un OTP. Eve intercepte le chiffré c et souhaite modifier le message de façon que si c'était un chiffré de "O" ça devienne un chiffré de "N" et inversement

Exercice sur terminal

Faites un `man xxd` dans un terminal pour voir comment transformer "O" et "N" en chaînes de bits

Comment doit-elle modifier c avant de le renvoyer ?

OTP : Malléabilité [2]

Contexte

Alice et Bob sont d'accord sur une clé, ils veulent s'échanger un message "O"ou "N" (pour oui et non) en utilisant un OTP. Eve intercepte le chiffré c et souhaite modifier le message de façon que si c'était un chiffré de "O" ça devienne un chiffré de "N" et inversement

Exercice sur terminal

Faites un `man xxd` dans un terminal pour voir comment transformer "O" et "N" en chaînes de bits

Comment doit-elle modifier c avant de le renvoyer ?

$c' = c \oplus (\text{“}O\text{”} \oplus \text{“}N\text{”}) = c \oplus 01001111 \oplus 01001110 = c \oplus 00000001$

OTP : Partage de secrets [2]

Partage à deux

Alice à un secret $x \in M$ qui permet de lancer des missiles nucléaires

Il génère $y \xleftarrow{U} M$ et donne :

- $x \oplus y$ à sa maman
- y à son papa

Maman et Papa pourront lancer la guerre nucléaire mais il faudra qu'il s'y mettent à deux

Quelles affirmations sont vraies ?

1. y suit une distribution uniforme sur M
2. $x \oplus y$ suit une distribution uniforme sur M
3. $(y, x \oplus y)$ suit une distribution uniforme sur $M \times M$

OTP : Partage de secrets [2]

Partage à deux

Alice à un secret $x \in M$ qui permet de lancer des missiles nucléaires

Il génère $y \xleftarrow{U} M$ et donne :

- $x \oplus y$ à sa maman
- y à son papa

Maman et Papa pourront lancer la guerre nucléaire mais il faudra qu'il s'y mettent à deux

Quelles affirmations sont vraies ?

1. y suit une distribution uniforme sur M
2. $x \oplus y$ suit une distribution uniforme sur M
3. $(y, x \oplus y)$ suit une distribution uniforme sur $M \times M$

OTP : Partage de secrets [2]

Partage à deux

Alice à un secret $x \in M$ qui permet de lancer des missiles nucléaires
Il génère $y \xleftarrow{U} M$ et donne :

- $x \oplus y$ à sa maman
- y à son papa

Maman et Papa pourront lancer la guerre nucléaire mais il faudra qu'il s'y mettent à deux

Alice veut faire un partage à 4 et x a cent bits de longueur

Combien de bits elle doit envoyer ?
Comment peut elle définir les secrets partagés ?

OTP : Généralisation avec des entiers

XOR $\Leftrightarrow$ mod 2 ... et pour des opérations mod p ?

Prennons $M = C = K = \mathbb{Z}_p^n$ et $sk \xleftarrow{U} \mathbb{Z}_p^n$

Questions

Comment définir les fonctions de chiffrement et déchiffrement ?
Développez un exemple avec des opérations par chiffre en base 10
Quelle distribution suivent les chiffrés ? Prouvez-le
Montrez que $P[X = m | Y = c] = P[X = m]$

Applications

OTP par caractère autre que binaire (décimal, hexadécimal)
OTP sur du texte directement

Pratique pour les humains uniquement !

OTP : Dining Cryptographers

Trois hurluberlus

... se retrouvent dans un restaurant. Soudainement, la serveuse apparaît et dit que le repas est payé. C'est l'un d'eux ou la NSA ?

David Chaum (1988). "The Dining Cryptographers Problem : Unconditional Sender and Recipient Untraceability". Journal of Cryptology 1 (1) : 65-75

Principe

A, B, C autour d'une table, chaque couple de voisins négocie un bit aléatoire

- A définit $m_A = 1$ s'il a payé, $m_A = 0$ s'il n'a pas payé
- A diffuse $d_A = m_A \oplus b_{AB} \oplus b_{AC}$, b_{XY} étant le bit partagé entre X et Y
- B et C suivent la même procédure
- Tout le monde calcule $r = d_A \oplus d_B \oplus d_C$

Questions (1/2)

Qu'est ce qu'ils font ?
Que vaut r ?
Que se passe-t-il s'ils sont deux à avoir payé ?
Généralisez le protocole pour qu'il marche avec des entiers, quel intérêt ?

OTP : Dining Cryptographers

Trois hurluberlus

... se retrouvent dans un restaurant. Soudainement, la serveuse apparaît et dit que le repas est payé. C'est l'un d'eux ou la NSA ?

David Chaum (1988). "The Dining Cryptographers Problem : Unconditional Sender and Recipient Untraceability". Journal of Cryptology 1 (1) : 65-75

Principe

A, B, C autour d'une table, chaque couple de voisins négocie un bit aléatoire

- A définit $m_A = 1$ s'il a payé, $m_A = 0$ s'il n'a pas payé
- A diffuse $d_A = m_A \oplus b_{AB} \oplus b_{AC}$, b_{XY} étant le bit partagé entre X et Y
- B et C suivent la même procédure
- Tout le monde calcule $r = d_A \oplus d_B \oplus d_C$

Questions (2/2)

Que faut-il pour qu'on sache ce que vaut m_A ?
Généralisez le protocole pour plus de 3 utilisateurs, qui est voisin de qui ?
Que faut-il de façon générale pour révéler m_A ?
Généralisez le protocole pour l'émission de plusieurs bits. Des applications ?

Défis

Défi : DC-nets

Faire un réseau de trois ordinateurs avec des secrets partagés
Utilisez les secrets comme graines de générateurs pseudo-aléatoires
Faire des tours du protocole DC toutes les milisecondes pour des messages de 1Ko
Trouver une application intéressante/rigolote à diffuser sur ce canal

Défi : Cryptanalyse

Écrivez un algorithme qui à partir de messages $m_1 \oplus m_2$ (en anglais) permet de séparer m_1 de m_2

Idée : ajoutez des petits mots du dictionnaire fréquents dans toutes les positions et voyez quand les compléments : sont des mots ; ont des enchaînements de lettre crédibles (bigrammes ou trigrammes habituels).

Fin

Prochain cours

Aléa, pseudo-aléa, et chiffrement à flots