Cryptologie et Sécurité: introduction

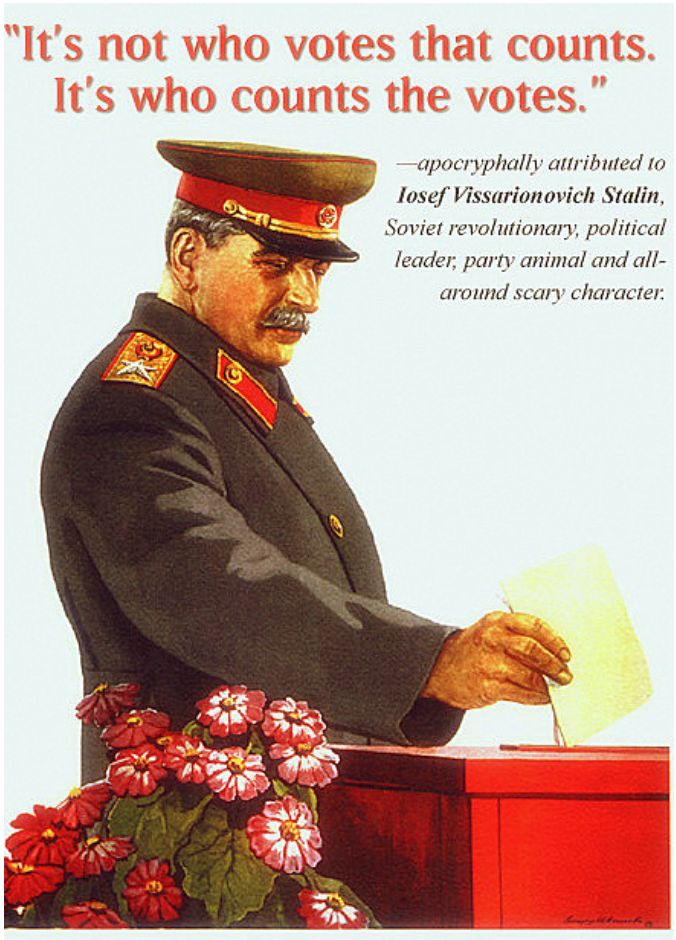
H. Comon

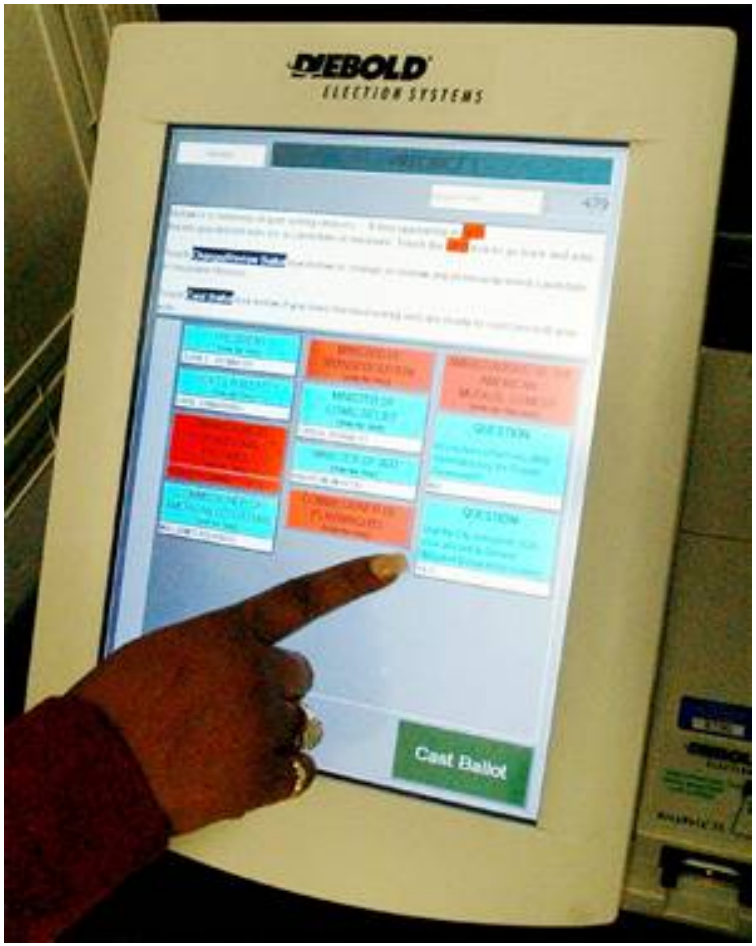
August 25, 2016

Sécurité informatique: enjeux (1)

- cartes de crédit
- cartes sans contact
- téléphones
- achats en ligne
- voitures et plus généralement internet des objets
- processus de fabrication
- Big Brother: le scandale NSA
- Biomédical
- ...

Sécurité informatique: enjeux (2)





Propriétés de sécurité

- Confidentialité
- Intégrité & Authenticité
- Respect de la vie privée

Comment assurer la sécurité ?

- Cryptographie:
  - Chiffrements
  - Signatures
  - Preuves à connaissance nulle
  - ...
- Protocoles (TLS, https,...)
- Contrôles d'accès
- Détection d'attaques

Chiffrement

- Chiffrement à clef secrète:
  Cesar, Enigma, **masque jetable**, Block ciphers (AES, DES), Stream ciphers
- Chiffrement à clef publique:
  Diffie Hellman, RSA, **El Gamal**,...

Propriétés requises:

- Chiffrer et déchiffrer doit être facile avec les clefs
- Déchiffrer doit être (très) difficile sans la clef.

Chiffrement de Cesar

Clef: décalage de 0 à 25.

Chiffrement: décaler toutes les lettres selon la clef

Exemple: $d = 6$,

`t` $\rightarrow$ `z`, `e` $\rightarrow$ `k`, `x` $\rightarrow$ `d`,...

`texte secret` $\rightarrow$ `zkdzk ykixkz`

Déchiffrement: décaler les lettres selon la clef, en sens inverse.

Attaques:

- Essayer toutes les clefs !
- Analyse de fréquence

Augmenter l'espace des clefs

Clef: permutation σ des 26 lettres. (Principe d'Enigma, qui comporte en plus des décalages et plusieurs tours)

Chiffrement: remplacer α par $\sigma(\alpha)$.

Exemple:

$$\sigma = \begin{pmatrix} \texttt{a} & \texttt{b} & \texttt{c} & \texttt{d} & \texttt{e} & \cdots & \texttt{r} & \texttt{s} & \texttt{t} & \cdots & \texttt{x} & \cdots \\ \texttt{j} & \texttt{w} & \texttt{a} & \texttt{u} & \texttt{c} & \cdots & \texttt{n} & \texttt{s} & \texttt{e} & \cdots & \texttt{h} & \cdots \end{pmatrix}$$

$$\texttt{texte secret} \quad \rightarrow$$

Augmenter l'espace des clefs

Clef: permutation σ des 26 lettres. (Principe d'Enigma, qui comporte en plus des décalages et plusieurs tours)

Chiffrement: remplacer α par $\sigma(\alpha)$.

Exemple:

$$\sigma = \begin{pmatrix} \texttt{a} & \texttt{b} & \texttt{c} & \texttt{d} & \texttt{e} & \cdots & \texttt{r} & \texttt{s} & \texttt{t} & \cdots & \texttt{x} & \cdots \\ \texttt{j} & \texttt{w} & \texttt{a} & \texttt{u} & \texttt{c} & \cdots & \texttt{n} & \texttt{s} & \texttt{e} & \cdots & \texttt{h} & \cdots \end{pmatrix}$$

$$\texttt{texte secret} \quad \rightarrow \quad \texttt{e}$$

Augmenter l'espace des clefs

Clef: permutation σ des 26 lettres. (Principe d'Enigma, qui comporte en plus des décalages et plusieurs tours)

Chiffrement: remplacer α par $\sigma(\alpha)$.

Exemple:

$$\sigma = \begin{pmatrix} \texttt{a} & \texttt{b} & \texttt{c} & \texttt{d} & \texttt{e} & \cdots & \texttt{r} & \texttt{s} & \texttt{t} & \cdots & \texttt{x} & \cdots \\ \texttt{j} & \texttt{w} & \texttt{a} & \texttt{u} & \texttt{c} & \cdots & \texttt{n} & \texttt{s} & \texttt{e} & \cdots & \texttt{h} & \cdots \end{pmatrix}$$

$$\texttt{texte secret} \quad \rightarrow \quad \texttt{ec}$$

Augmenter l'espace des clefs

Clef: permutation σ des 26 lettres. (Principe d'Enigma, qui comporte en plus des décalages et plusieurs tours)

Chiffrement: remplacer α par $\sigma(\alpha)$.

Exemple:

$$\sigma = \begin{pmatrix} \texttt{a} & \texttt{b} & \texttt{c} & \texttt{d} & \texttt{e} & \cdots & \texttt{r} & \texttt{s} & \texttt{t} & \cdots & \texttt{x} & \cdots \\ \texttt{j} & \texttt{w} & \texttt{a} & \texttt{u} & \texttt{c} & \cdots & \texttt{n} & \texttt{s} & \texttt{e} & \cdots & \texttt{h} & \cdots \end{pmatrix}$$

$$\texttt{texte secret} \quad \rightarrow \quad \texttt{ech}$$

Augmenter l'espace des clefs

Clef: permutation σ des 26 lettres. (Principe d'Enigma, qui comporte en plus des décalages et plusieurs tours)

Chiffrement: remplacer α par $\sigma(\alpha)$.

Exemple:

$$\sigma = \begin{pmatrix} \texttt{a} & \texttt{b} & \texttt{c} & \texttt{d} & \texttt{e} & \cdots & \texttt{r} & \texttt{s} & \texttt{t} & \cdots & \texttt{x} & \cdots \\ \texttt{j} & \texttt{w} & \texttt{a} & \texttt{u} & \texttt{c} & \cdots & \texttt{n} & \texttt{s} & \texttt{e} & \cdots & \texttt{h} & \cdots \end{pmatrix}$$

$$\texttt{texte secret} \quad \rightarrow \quad \texttt{eche}$$

Augmenter l'espace des clefs

Clef: permutation σ des 26 lettres. (Principe d'Enigma, qui comporte en plus des décalages et plusieurs tours)

Chiffrement: remplacer α par $\sigma(\alpha)$.

Exemple:

$$\sigma = \begin{pmatrix} \texttt{a} & \texttt{b} & \texttt{c} & \texttt{d} & \texttt{e} & \cdots & \texttt{r} & \texttt{s} & \texttt{t} & \cdots & \texttt{x} & \cdots \\ \texttt{j} & \texttt{w} & \texttt{a} & \texttt{u} & \texttt{c} & \cdots & \texttt{n} & \texttt{s} & \texttt{e} & \cdots & \texttt{h} & \cdots \end{pmatrix}$$

$$\texttt{texte secret} \quad \rightarrow \quad \texttt{echec}$$

Augmenter l'espace des clefs

Clef: permutation σ des 26 lettres. (Principe d'Enigma, qui comporte en plus des décalages et plusieurs tours)

Chiffrement: remplacer α par $\sigma(\alpha)$.

Exemple:

$$\sigma = \begin{pmatrix} \texttt{a} & \texttt{b} & \texttt{c} & \texttt{d} & \texttt{e} & \cdots & \texttt{r} & \texttt{s} & \texttt{t} & \cdots & \texttt{x} & \cdots \\ \texttt{j} & \texttt{w} & \texttt{a} & \texttt{u} & \texttt{c} & \cdots & \texttt{n} & \texttt{s} & \texttt{e} & \cdots & \texttt{h} & \cdots \end{pmatrix}$$

$$\texttt{texte secret} \quad \rightarrow \quad \texttt{echec s}$$

Augmenter l'espace des clefs

Clef: permutation σ des 26 lettres. (Principe d'Enigma, qui comporte en plus des décalages et plusieurs tours)

Chiffrement: remplacer α par $\sigma(\alpha)$.

Exemple:

$$\sigma = \begin{pmatrix} \texttt{a} & \texttt{b} & \texttt{c} & \texttt{d} & \texttt{e} & \cdots & \texttt{r} & \texttt{s} & \texttt{t} & \cdots & \texttt{x} & \cdots \\ \texttt{j} & \texttt{w} & \texttt{a} & \texttt{u} & \texttt{c} & \cdots & \texttt{n} & \texttt{s} & \texttt{e} & \cdots & \texttt{h} & \cdots \end{pmatrix}$$

$$\texttt{texte secret} \quad \rightarrow \quad \texttt{echec sc}$$

Augmenter l'espace des clefs

Clef: permutation σ des 26 lettres. (Principe d'Enigma, qui comporte en plus des décalages et plusieurs tours)

Chiffrement: remplacer α par $\sigma(\alpha)$.

Exemple:

$$\sigma = \begin{pmatrix} \texttt{a} & \texttt{b} & \texttt{c} & \texttt{d} & \texttt{e} & \cdots & \texttt{r} & \texttt{s} & \texttt{t} & \cdots & \texttt{x} & \cdots \\ \texttt{j} & \texttt{w} & \texttt{a} & \texttt{u} & \texttt{c} & \cdots & \texttt{n} & \texttt{s} & \texttt{e} & \cdots & \texttt{h} & \cdots \end{pmatrix}$$

$$\texttt{texte secret} \quad \rightarrow \quad \texttt{echec scince}$$

Augmenter l'espace des clefs

Clef: permutation σ des 26 lettres. (Principe d'Enigma, qui comporte en plus des décalages et plusieurs tours)

Chiffrement: remplacer α par $\sigma(\alpha)$.

Exemple:

$$\sigma = \begin{pmatrix} \texttt{a} & \texttt{b} & \texttt{c} & \texttt{d} & \texttt{e} & \cdots & \texttt{r} & \texttt{s} & \texttt{t} & \cdots & \texttt{x} & \cdots \\ \texttt{j} & \texttt{w} & \texttt{a} & \texttt{u} & \texttt{c} & \cdots & \texttt{n} & \texttt{s} & \texttt{e} & \cdots & \texttt{h} & \cdots \end{pmatrix}$$

$$\texttt{texte secret} \quad \rightarrow \quad \texttt{echec scince}$$

Déchiffrement: remplacer α par $\sigma^{-1}(\alpha)$.

Attaques

- Analyse de fréquence
- Problème du clair connu: Sachant que $\sigma(\texttt{secret}) = \texttt{scince}$, $\sigma(\texttt{s}) = \texttt{s}, \sigma(\texttt{e}) = \texttt{c}, \sigma(\texttt{t}) = \texttt{e}$
  $\sigma^{-1}(\texttt{echec}) = \texttt{te?te}$

Enigma

Chiffrement:
Permutations + décalages

Attaques:
analyse de fréquence (de suites de lettres), clair connu ...

Remarque:
le secret du procédé est illusoire

Sécurité du chiffrement

Ce dont dispose l'attaquant: plusieurs modèles

- Plusieurs chiffrés
- Clair connu: plusieurs paires (texte en clair, texte chiffré)
- Clair choisi: plusieurs paires (texte en clair, texte chiffré) dans lesquelles le texte en clair est au choix de l'attaquant.
- Chiffré choisi: accès supplémentaire à un oracle de déchiffrement

Plusieurs définitions du succès de l'attaquant:

- L'attaquant calcule la clef de déchiffrement
- L'attaquant calcule le texte en clair
- L'attaquant calcule une partie du texte en clair
- L'attaquant peut distinguer deux textes en clairs chiffrés de son choix

One time pad

Masque jetable

Chiffrement d'un mot w

- tirer aléatoirement un mot k de même longueur que w
- Le chiffré est $c = w \oplus k$. (On suppose pour simplifier que w et k sont en binaire).

Déchiffrement

$w = c \oplus k$

$$\begin{array}{c} 11111100000 \\ \oplus \\ 10101100010 \\ = \\ 01010000010 \end{array} \qquad \begin{array}{c} 01010000010 \\ \oplus \\ 10101100010 \\ = \\ 11111100000 \end{array}$$

Théorème de Shannon

Théorème

1. Si la clef k est tirée uniformément à chaque chiffrement, alors le masque jetable est un chiffrement parfaitement sûr.
2. Il n'y a aucun autre chiffrement qui soit parfaitement sûr.

Théorème de Shannon

Théorème

1. Si la clef k est tirée uniformément à chaque chiffrement, alors le masque jetable est un chiffrement parfaitement sûr.
2. Il n'y a aucun autre chiffrement qui soit parfaitement sûr.

Difficultés:

- se mettre d'accord sur les clefs.
- problème des longueurs de clefs.
- générateur aléatoire ?

Théorème de Shannon

Théorème

1. Si la clef k est tirée uniformément à chaque chiffrement, alors le masque jetable est un chiffrement parfaitement sûr.
2. Il n'y a aucun autre chiffrement qui soit parfaitement sûr.

Difficultés:

- se mettre d'accord sur les clefs.
- problème des longueurs de clefs.
- générateur aléatoire ?

Définition de la sécurité probabiliste

Échange de clefs

Échange de lettres d'amour

Échange de clefs

Échange de lettres d'amour

Échange de secrets (2)

1. Alice envoie ses secrets dans un coffre fermé avec son cadenas

Échange de secrets (2)

1. Alice envoie ses secrets dans un coffre fermé avec son cadenas
2. Bob ajoute son propre cadenas au coffre et renvoie à Alice

Échange de secrets (2)

1. Alice envoie ses secrets dans un coffre fermé avec son cadenas
2. Bob ajoute son propre cadenas au coffre et renvoie à Alice
3. Alice retire son cadenas et renvoie à Bob

Problème d'authenticité

"Man in the middle attack"

1. Alice envoie ses secrets dans un coffre fermé avec son cadenas

Problème d'authenticité

"Man in the middle attack"

1. Alice envoie ses secrets dans un coffre fermé avec son cadenas
2. Charlie intercepte, ajoute son propre cadenas et renvoie à Alice

Problème d'authenticité

"Man in the middle attack"

1. Alice envoie ses secrets dans un coffre fermé avec son cadenas
2. Charlie intercepte, ajoute son propre cadenas et renvoie à Alice
3. Alice retire son cadenas et renvoie à Bob

Problème d'authenticité

"Man in the middle attack"

1. Alice envoie ses secrets dans un coffre fermé avec son cadenas
2. Charlie intercepte, ajoute son propre cadenas et renvoie à Alice
3. Alice retire son cadenas et renvoie à Bob
4. Charlie intercepte, retire son cadenas, copie le contenu du coffre, remet son cadenas et envoie à Bob

Problème d'authenticité

"Man in the middle attack"

1. Alice envoie ses secrets dans un coffre fermé avec son cadenas
2. Charlie intercepte, ajoute son propre cadenas et renvoie à Alice
3. Alice retire son cadenas et renvoie à Bob
4. Charlie intercepte, retire son cadenas, copie le contenu du coffre, remet son cadenas et envoie à Bob
5. Bob ajoute son propre cadenas au coffre et renvoie à Alice

Problème d'authenticité

"Man in the middle attack"

1. Alice envoie ses secrets dans un coffre fermé avec son cadenas
2. Charlie intercepte, ajoute son propre cadenas et renvoie à Alice
3. Alice retire son cadenas et renvoie à Bob
4. Charlie intercepte, retire son cadenas, copie le contenu du coffre, remet son cadenas et envoie à Bob
5. Bob ajoute son propre cadenas au coffre et renvoie à Alice
6. Charlie intercepte, retire son cadenas et renvoie à Bob

Problème d'authenticité

"Man in the middle attack"

1. Alice envoie ses secrets dans un coffre fermé avec son cadenas
2. Charlie intercepte, ajoute son propre cadenas et renvoie à Alice
3. Alice retire son cadenas et renvoie à Bob
4. Charlie intercepte, retire son cadenas, copie le contenu du coffre, remet son cadenas et envoie à Bob
5. Bob ajoute son propre cadenas au coffre et renvoie à Alice
6. Charlie intercepte, retire son cadenas et renvoie à Bob

Il faut un moyen de s'assurer qu'un cadenas appartient bien à Alice.

Échange de clefs de Diffie-Hellman

p nombre premier
$G_p = (\mathbb{Z}/p\mathbb{Z})^*$ groupe multiplicatif de générateur g. (p, g sont publics).

1. a choisit une clef secrète $x \in G_p$ et envoie $g^x \mod p$
2. b choisit une clef secrète $y \in G_p$ et envoie $g^y \mod p$
3. a calcule

$$(g^y)^x \mod p = g^{x \times y} \mod p = (g^x)^y \mod p$$

que calcule b

$g^{x \times y} \mod p$ est la clef partagée.

Sécurité: repose sur la difficulté supposée du logarithme discret. Suppose un mécanisme d'authentification.

Exponentiation rapide

Si p est de l'ordre de 2^{512}, g, x aussi, comment effectuer efficacement le calcul de $g^x \mod p$?

Exponentiation rapide

Si p est de l'ordre de 2^{512}, g, x aussi, comment effectuer efficacement le calcul de $g^x \mod p$?

Remarquer que

$g^{x0} = (g^x)^2$ et $g^{x1} = (g^x)^2 \times g$.

Autrement dit: on a besoin de l'ordre de 512 multiplications et non 2^{512} multiplications comme dans la méthode naïve.

Chiffrement El Gamal

p premier, g générateur de G_p, $g^{k_a} \mod p$, $g^{k_b} \mod p$ sont publics.

Chiffrement El Gamal

p premier, g générateur de G_p, $g^{k_a} \mod p$, $g^{k_b} \mod p$ sont publics.

Chiffrement à destination de b du message $m \in G_p$:

- tirer aléaoirement $r \in G_p$
- envoyer $\left\langle g^r \mod p, m \times g^{k_b \times r} \mod p \right\rangle$

Chiffrement El Gamal

p premier, g générateur de G_p, $g^{k_a} \mod p$, $g^{k_b} \mod p$ sont publics.

Chiffrement à destination de b du message $m \in G_p$:

- tirer aléaoirement $r \in G_p$
- envoyer $\left\langle g^r \mod p, m \times g^{k_b \times r} \mod p \right\rangle$

Déchiffrement par b à réception de $\langle x, y \rangle$:

- élever x à la puissance $p - 1 - k_b \pmod p$
- multiplier y par le résultat $\pmod p$

$$g^{r \times (p-1-k_b)} \times m \times g^{k_b \times r} = m \times g^{r \times (p-1)} = m \mod p$$

Chiffrement El Gamal

p premier, g générateur de G_p, $g^{k_a} \mod p$, $g^{k_b} \mod p$ sont publics.

Chiffrement à destination de b du message $m \in G_p$:

- tirer aléaoirement $r \in G_p$
- envoyer $\left\langle g^r \mod p, m \times g^{k_b \times r} \mod p \right\rangle$

Déchiffrement par b à réception de $\langle x, y \rangle$:

- élever x à la puissance $p - 1 - k_b \pmod p$
- multiplier y par le résultat $\pmod p$

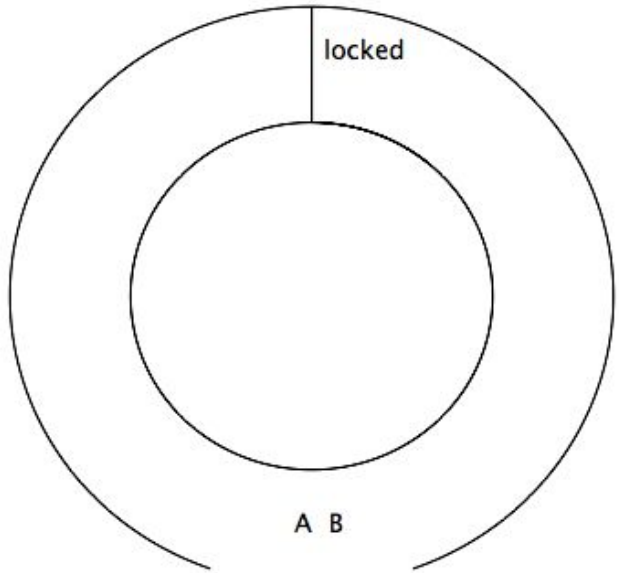
$$g^{r \times (p-1-k_b)} \times m \times g^{k_b \times r} = m \times g^{r \times (p-1)} = m \mod p$$

Sécurité (à clair choisi) basée sur la difficulté du logarithme discret.

Signatures

- La clef de signature est secrete
- La clef de vérification est publique

Preuves à divulgation nulle



Protocoles

Exemple du postier

$$\begin{aligned} A \to B : &\quad \mathrm{enc}(s, k_a) \\ B \to A &\quad \mathrm{enc}(\mathrm{enc}(s, k_a), k_b) \\ A \to B &\quad \mathrm{enc}(s, k_a) \end{aligned}$$

Le modèle de Dolev-Yao

- L'attaquant peut intercepter, modifier et émettre des messages
- L'attaquant ne peut pas déchiffrer ou modifier le message clair d'un chiffré, sans posséder la clef de déchiffrement.

Protocole: détail

$$A(a) = \mathsf{out}(\mathsf{enc}(s, k_a));\ \mathsf{in}(\mathsf{enc}(X, k_a));\ \mathsf{out}(X);$$

$$A \to B \quad \mathsf{enc}(s, k_a)$$
$$B \to A : \ \mathsf{enc}(\mathsf{enc}(s, k_a), k_b)$$
$$A \to B : \ \mathsf{enc}(s, k_b)$$

$$B(b) = \mathsf{in}(Y);\ \mathsf{out}(\mathsf{enc}(Y, k_b));\ \mathsf{in}(\mathsf{enc}(Z, k_b));$$

$$A \to B \quad \mathsf{enc}(s, k_a)$$
$$B \to A : \ \mathsf{enc}(\mathsf{enc}(s, k_a), k_b)$$
$$A \to B : \ \mathsf{enc}(s, k_b)$$

Protocole: détail

$$A(a) = \text{out}(\text{enc}(s, k_a);\ \text{in}(\text{enc}(X, k_a));\ \text{out}(X);$$

$$A \to B \quad \text{enc}(s, k_a)$$
$$B \to A: \quad \text{enc}(\text{enc}(s, k_a), k_b)$$
$$A \to B: \quad \text{enc}(s, k_b)$$

$$B(b) = \text{in}(Y);\ \text{out}(\text{enc}(Y, k_b));\ \text{in}(\text{enc}(Z, k_b));$$

$$A \to B \quad \text{enc}(s, k_a)$$
$$B \to A: \quad \text{enc}(\text{enc}(s, k_a), k_b)$$
$$A \to B: \quad \text{enc}(s, k_b)$$

Attaque

$$\begin{array}{lll} A \to & \text{enc}(s, k_a) & \\ A \leftarrow & \text{enc}(\text{enc}(s, k_a), k_c) & X = \text{enc}(s, k_c) \\ A \to & \text{enc}(s, k_c) & \\ \to B & \text{enc}(s, k_c) & Y = \text{enc}(s, k_c) \\ \leftarrow B & \text{enc}(\text{enc}(s, k_c), k_b) & \\ \to B & \text{enc}(s, k_b) & Z = s \end{array}$$

Autres problèmes de sécurité

- Certification
- Virus, chevaux de Troie & vers informatique
- Stenographie, canaux subliminaux
- Attaques par canaux auxilliaires
- Déni de service
- Phishing
- Intrusions
- ...

Pour en savoir plus

Livres

- J. Stern, *La science du secret*
- B. Schneier, *Cryptographie appliquée*

Videos

- Cours au collège de France: Martìn Abadi
- Parmi les milliers de videos, celles des collègues proches: Anne Canteaut, Graham Steel, Daniel Augot, ...

Binaire

Plusieurs articles, en particulier de Stéphanie Delaune (bitcoin) et Véronique Cortier (vote électronique).

Ressources en ligne

`Dcode`

Activités reliées au collège ?

- Jeux chiffrement vs cryptanalyse ?
- Algorithmique des nombres ?
- Sténographie ?