Cryptographie : Cryptographie à clé publique

JOHRI Mustapha

ESTBM

Introduction

- Considérons deux ensembles X et Y et une fonction $f : X \to Y$.

Introduction

- Considérons deux ensembles X et Y et une fonction $f : X \to Y$.
- La fonction f est dite à **sens unique** si $\forall x \in X$ il est facile de calculer $f(x)$ et s'il est difficile de trouver pour la plupart des $y \in f(X)$ un $x \in X$ tel que $f(x) = y$

Introduction

- Considérons deux ensembles X et Y et une fonction $f : X \to Y$.
- La fonction f est dite à **sens unique** si $\forall x \in X$ il est facile de calculer $f(x)$ et s'il est difficile de trouver pour la plupart des $y \in f(X)$ un $x \in X$ tel que $f(x) = y$
- Les fonctions à sens unique **ne peuvent pas servir** telles quelles de **système de chiffrement** puisque même le destinataire légal ne serait pas en mesure de déchiffrer le cryptogramme.

Introduction

- Considérons deux ensembles X et Y et une fonction $f : X \to Y$.
- La fonction f est dite à **sens unique** si $\forall x \in X$ il est facile de calculer $f(x)$ et s'il est difficile de trouver pour la plupart des $y \in f(X)$ un $x \in X$ tel que $f(x) = y$
- Les fonctions à sens unique **ne peuvent pas servir** telles quelles de **système de chiffrement** puisque même le destinataire légal ne serait pas en mesure de déchiffrer le cryptogramme.
- La solution est d'utiliser des fonctions à sens unique à **trappe**

Introduction

- Considérons deux ensembles X et Y et une fonction $f : X \to Y$.
- La fonction f est dite à **sens unique** si $\forall x \in X$ il est facile de calculer $f(x)$ et s'il est difficile de trouver pour la plupart des $y \in f(X)$ un $x \in X$ tel que $f(x) = y$
- Les fonctions à sens unique **ne peuvent pas servir** telles quelles de **système de chiffrement** puisque même le destinataire légal ne serait pas en mesure de déchiffrer le cryptogramme.
- La solution est d'utiliser des fonctions à sens unique à **trappe**
- Une fonction $f : X \to Y$ est **dite à trappe** si elle peut être calculée **efficacement** dans le **sens direct**. Le calcul dans le sens **inverse** est aussi efficace pourvu qu'on **dispose** d'une **information secrète**, **la trappe**, qui permette de construire une fonction g telle que $g \circ f = Id$

Sac à dos Merkle–Hellman

Sac à dos Merkle–Hellman : Présentation

- Un problème est **calculatoirement difficile** s'il n'existe pas d'algorithme de résolution de ce problème en temps raisonnable.

Sac à dos Merkle–Hellman : Présentation

- Un problème est **calculatoirement difficile** s'il n'existe pas d'algorithme de résolution de ce problème en temps raisonnable.

Exemple

Donnée *: Un ensemble A de n entiers $A = (a_1, \dots, a_n)$ tels que les a_i sont tous distincts et un entier k.*
Question *: Existe-t-il un sous-ensemble de A dont la somme est égale à k ?*

Exemple :
pour $A = (43, 129, 215, 473, 903, 302, 561, 1165, 697, 1523)$ et
$k = 3231$,
on remarque que $3231 = 129 + 473 + 903 + 561 + 1165$ est solution.

Sac à dos Merkle–Hellman : Présentation

- Un problème est **calculatoirement difficile** s'il n'existe pas d'algorithme de résolution de ce problème en temps raisonnable.

Exemple

Donnée *: Un ensemble A de n entiers $A = (a_1, ..., a_n)$ tels que les a_i sont tous distincts et un entier k.*
Question *: Existe-t-il un sous-ensemble de A dont la somme est égale à k ?*

Exemple :
pour $A = (43, 129, 215, 473, 903, 302, 561, 1165, 697, 1523)$ et $k = 3231$,
on remarque que $3231 = 129 + 473 + 903 + 561 + 1165$ est solution.

- pour $n = 300$ sur une machine qui effectue un million d'opération par seconde, il faudrait 6.4×10^{76} secondes de temps de calcul !

Fonction à sens unique

Le problème consiste à définir une fonction à sens unique comme suit :

- $\forall x, 0 \leq x \leq 2^n - 1$ admet une unique représentation en binaire sur n bits
- $f(x)$ le nombre obtenu à partir des entiers de A, en sommant les a_i pour lesquells le bit x_i est égale à 1
-

$$
\begin{aligned}
f(1) &= f(0...01) = \langle A, 0...01 \rangle = a_n \\
f(2) &= f(0...10) = \langle A, 0...10 \rangle = a_{n-1} \\
f(3) &= f(0...11) = \langle A, 0...11 \rangle = a_n + a_{n-1} \\
&\dots
\end{aligned}
$$

Exercice

Pour $A = (43, 129, 215, 473, 903, 302, 561, 1165, 697, 1523)$ *avec* $n = 10$, *calculer* $f(364)$ *?*

Fonction à sens unique

Le problème consiste à définir une fonction à sens unique comme suit :

- $\forall x, 0 \leq x \leq 2^n - 1$ admet une unique représentation en binaire sur n bits
- $f(x)$ le nombre obtenu à partir des entiers de A, en sommant les a_i pour lesquells le bit x_i est égale à 1
-
$$
\begin{aligned}
f(1) &= f(0...01) = \langle A, 0...01 \rangle = a_n \\
f(2) &= f(0...10) = \langle A, 0...10 \rangle = a_{n-1} \\
f(3) &= f(0...11) = \langle A, 0...11 \rangle = a_n + a_{n-1} \\
&\dots
\end{aligned}
$$

Exercice

Pour $A = (43, 129, 215, 473, 903, 302, 561, 1165, 697, 1523)$ *avec* $n = 10$, *calculer* $f(364)$ *?*

$f(364) = f(0101101100) = 129 + 473 + 903 + 561 + 1165 = 3231$

Fonction à sens unique

- Pour **chiffrer** on applique f sur des blocs de n bits correspondants à une suite de bits du texte clair

Exemple

Si on code a par $1 = 00001$*...z par* $26 = 11010$ *on peut coder par concaténation deux caractères sur 10 bits. Sur le texte* ***qui dort dine*** *on obtient :*

qu	*i*	*do*	*rt*	*d*	*in*	*e*
1000110101	*0100100000*	..	..	..	..	..
(3936	*1032*	*4161*	*1983*	*1165*	*3455*	*1118)*

Transformation en un système à clé publique

Transformation en un système à clé publique

- Le destinataire choisit un ensemble A forment une suite appelée **super-croissante** qui verifie : $\sum_{i=1}^{j-1} a_i < a_j, \ \forall j, 1 < j \leq n,.$
- Avec cet ensemble, le problème précédent admet une solution **facile**.

Transformation en un système à clé publique

- Le destinataire choisit un ensemble A forment une suite appelée **super-croissante** qui verifie : $\sum_{i=1}^{j-1} a_i < a_j, \ \forall j, 1 < j \leq n,$.
- Avec cet ensemble, le problème précédent admet une solution **facile**.
  - En effet, il suffit de parcourir A de la droite vers la gauche ($\leftarrow$) de la façon suivante : étant donné k, on compare k et a_n.
  - Si $a_n > k, \ a_n$ n'est pas dans la somme et on passe à l'élément a_{n-1},
  - Si $a_n \leq k$, alors a_n est dans la somme et on recommence avec la valeur $k_1 = k - a_n \geq a_{n-1}$?

Transformation en un système à clé publique

- Le destinataire choisit un ensemble A forment une suite appelée **super-croissante** qui verifie : $\sum_{i=1}^{j-1} a_i < a_j, \ \forall j, 1 < j \leq n,$.
- Avec cet ensemble, le problème précédent admet une solution **facile**.
  - En effet, il suffit de parcourir A de la droite vers la gauche $(\leftarrow)$ de la façon suivante : étant donné k, on compare k et a_n.
  - Si $a_n > k, \ a_n$ n'est pas dans la somme et on passe à l'élément a_{n-1},
  - Si $a_n \leq k$, alors a_n est dans la somme et on recommence avec la valeur $k_1 = k - a_n \geq a_{n-1}$?
  - Cet algorithme se termine quand on a atteint l'élément a_1.
- Pour chaque entier k, le problème correspondant a au plus une solution.

Transformation en un système à clé publique

- Le destinataire choisit un ensemble A forment une suite appelée **super-croissante** qui verifie : $\sum_{i=1}^{j-1} a_i < a_j, \ \forall j, 1 < j \leq n,$.
- Avec cet ensemble, le problème précédent admet une solution **facile**.
  - En effet, il suffit de parcourir A de la droite vers la gauche ($\leftarrow$) de la façon suivante : étant donné k, on compare k et a_n.
  - Si $a_n > k, \ a_n$ n'est pas dans la somme et on passe à l'élément a_{n-1},
  - Si $a_n \leq k$, alors a_n est dans la somme et on recommence avec la valeur $k_1 = k - a_n \geq a_{n-1}$?
  - Cet algorithme se termine quand on a atteint l'élément a_1.
- Pour chaque entier k, le problème correspondant a au plus une solution.
- Si **on publie** A, **déchiffrer sera aussi facile** pour le destinataire que pour un cryptanalyste !

Transformation en un système à clé publique

- Le destinataire choisit un ensemble A forment une suite appelée **super-croissante** qui verifie : $\sum_{i=1}^{j-1} a_i < a_j, \ \forall j, 1 < j \leq n,$.
- Avec cet ensemble, le problème précédent admet une solution **facile**.
  - En effet, il suffit de parcourir A de la droite vers la gauche ($\leftarrow$) de la façon suivante : étant donné k, on compare k et a_n.
  - Si $a_n > k$, a_n n'est pas dans la somme et on passe à l'élément a_{n-1},
  - Si $a_n \leq k$, alors a_n est dans la somme et on recommence avec la valeur $k_1 = k - a_n \geq a_{n-1}$?
  - Cet algorithme se termine quand on a atteint l'élément a_1.
- Pour chaque entier k, le problème correspondant a au plus une solution.
- Si **on publie** A, **déchiffrer sera aussi facile** pour le destinataire que pour un cryptanalyste !
- **On va perturber** A en un ensemble B de telle sorte que le n-uplet résultant ressemble à un ensemble arbitraire.

Perturbation de l'ensemble

- Pour **perturber** A, on utilise une **multiplication modulaire** en arithmétique modulo $m > \sum_{i=1}^{n} a_i$.

Perturbation de l'ensemble

- Pour **perturber** A, on utilise une **multiplication modulaire** en arithmétique modulo $m > \sum_{i=1}^{n} a_i$.
- On va choisir un autre entier t premier avec m $(pgcd(t, m) = 1)$
- Pour tout $i, 1 \leq i \leq n$ et on obtient un nouveau ensemble B formé par les produits $b_i = a_i \times t \mod m$, qui est utilisé comme **clé publique**

Perturbation de l'ensemble

- Pour **perturber** A, on utilise une **multiplication modulaire** en arithmétique modulo $m > \sum_{i=1}^{n} a_i$.
- On va choisir un autre entier t premier avec m $(pgcd(t, m) = 1)$
- Pour tout $i, 1 \leq i \leq n$ et on obtient un nouveau ensemble B formé par les produits $b_i = a_i \times t \mod m$, qui est utilisé comme **clé publique**
- les entiers t, t^{-1}, m et A constituent **la clé secrète** (la trappe).

Perturbation de l'ensemble

- Pour **perturber** A, on utilise une **multiplication modulaire** en arithmétique modulo $m > \sum_{i=1}^{n} a_i$.
- On va choisir un autre entier t premier avec m ($pgcd(t, m) = 1$)
- Pour tout $i, 1 \leq i \leq n$ et on obtient un nouveau ensemble B formé par les produits $b_i = a_i \times t \;\; mod \;\; m$, qui est utilisé comme **clé publique**
- les entiers t, t^{-1}, m et A constituent **la clé secrète** (la trappe).
- Ainsi pour **chiffrer** un message binaire M de n bits, on calcul $c = \langle B, M \rangle$

Perturbation de l'ensemble

Exemple

Un destinataire choisit l'ensemble $A = (1, 3, 5, 11, 21, 44, 87, 175, 349, 701)$ *et les paramètres* $m = 1590$, $t = 43$. *Vérifier qu'il s'agit d'un cryptosystème de Merkle-Hellman et précisant la clé publique et privée ? chiffrer le mot* ***"GI"*** *?*

Perturbation de l'ensemble

Exemple

Un destinataire choisit l'ensemble $A = (1, 3, 5, 11, 21, 44, 87, 175, 349, 701)$ *et les paramètres* $m = 1590,\ t = 43$. *Vérifier qu'il s'agit d'un cryptosystème de Merkle-Hellman et précisant la clé publique et privée ? chiffrer le mot* ***"GI"*** *?*

A est bien une suite super-croissante et l'inverse de t modulo m est $t^{-1} = 37$.
Alors la clé publique est :
$B = (43, 129, 215, 473, 903, 302, 561, 1165, 697, 1523)$ *et on garde* A, m, t, t^{-1} *comme clé secrète.*
"GI" $\rightarrow 00111\,01001$, *alors :*

$$c = \langle B, 0011101001 \rangle = 3675$$

Comment déchiffrer ?

- Après avoir reçu un bloc chiffré $c \in \mathbb{N}$, il calcul $t^{-1}c = x \ \ mod \ \ m$
- la solution définit une suite unique M de n bits. il s'agit aussi d'un bloc du clair

$$x \equiv t^{-1}c \equiv t^{-1}\langle B, c\rangle \equiv t^{-1}t\langle A, c\rangle \equiv \langle A, c\rangle \ \ mod \ \ m$$

Comment déchiffrer ?

- Après avoir reçu un bloc chiffré $c \in \mathbb{N}$, il calcul $t^{-1}c = x \ \ mod \ \ m$
- la solution définit une suite unique M de n bits. il s'agit aussi d'un bloc du clair

$$x \equiv t^{-1}c \equiv t^{-1}\langle B, c\rangle \equiv t^{-1}t\langle A, c\rangle \equiv \langle A, c\rangle \ \ mod \ \ m$$

Exemple

Déchiffrons pas exemple le cryptogramme

$$(3936, 1032, 4161, 1983, 1165, 3455, 1118)$$

Comment déchiffrer ?

- Après avoir reçu un bloc chiffré $c \in \mathbb{N}$, il calcul $t^{-1}c = x \mod m$
- la solution définit une suite unique M de n bits. il s'agit aussi d'un bloc du clair

$$x \equiv t^{-1}c \equiv t^{-1}\langle B, c\rangle \equiv t^{-1}t\langle A, c\rangle \equiv \langle A, c\rangle \mod m$$

Exemple

Déchiffrons pas exemple le cryptogramme

$$(3936, 1032, 4161, 1983, 1165, 3455, 1118)$$

On multiplie par $t^{-1} = 37$ *modulo* m *avec* $m = 1590$*. on obtient* $(942, 24, 1317, 231, 175, 635, 26)$, *Déchiffrons seulement le bloc 942 avec la suite super-croissante* $A = (1, 3, 5, 11, 21, 44, 87, 175, 349, 701)$

- $M = 100010101$ *qui correspond au bloc de deux lettre* ***qu***