Chiffrement à clés publiques

Vincent Vajnovszki

Clé secrète:

- Principe de Auguste Kerckhoffs : *la sécurité d'un cryptosystème doit reposer uniquement sur le secret de la clef*

Clé secrète:

- Principe de Auguste Kerckhoffs : *la sécurité d'un cryptosystème doit reposer uniquement sur le secret de la clef*

"principe qui résume d'ailleurs toute ma thèse, à savoir qu'un chiffre n'est bon qu'autant qu'il reste indéchiffrable pour le maître lui-même qui l'a inventé : Ars ipsi secreta magistro."

Clé secrète:

- Principe de Auguste Kerckhoffs : *la sécurité d'un cryptosystème doit reposer uniquement sur le secret de la clef*

"principe qui résume d'ailleurs toute ma thèse, à savoir qu'un chiffre n'est bon qu'autant qu'il reste indéchiffrable pour le maître lui-même qui l'a inventé : Ars ipsi secreta magistro."

- Claude Shannon : *l'adversaire connaît le système*
- Autrement dit : *tous les autres paramètres doivent être supposés publiquement connus; s'oppose à la sécurité par l'obscurité*

Limitations de la cryptographie à clé secrète:

- la clé doit rester secrète
- communication de la clé : valise diplomatique
- explosion des communications : nombre de clés secrètes augmentent
- problème d'authentification : un utilisateur s'envoie un message fictif au nom de son correspondant. Falsification non prouvable (même clé) !

- Après la Seconde Guerre Mondiale, l'échange de clés est la principale faille de sécurité en cryptographie.
- Résultat : les corps diplomatiques dépensent des sommes folles juste pour acheminer des clés secrètes d'agent secret à agent secret.
- Absurde ? Pas tant que ça, si on considère la facilité avec laquelle on peut ouvrir l'air de rien une enveloppe à la vapeur. Et, tant qu'une clé n'est pas précisée entre Alice et Bob, impossible d'envoyer un message codé. Ce casse-tête va notamment passionner les chercheurs.

Idée saugrenue : Cherchons un moyen de communiquer sans qu'il y ait besoin de s'échanger une clé secrète...
Réaction de la communauté cryptographique de l'époque : mitigée

Idée d'une nouvelle méthode

Idée faisable physiquement :

Alice et Bob veulent communiquer, mais ne se sont pas mis d'accord sur un secret commun. Comment peuvent-ils communiquer ?

C'est possible !

James Ellis, cryptographe des services britanniques, comprend que la distribution des clés n'est pas inévitable.

Le protocole :

- le receveur masque les paroles de son interlocuteur, en ajoutant du bruit sur la ligne téléphonique;
- comme c'est le receveur qui a créé ce bruit et l'a ajouté, il peut ensuite le soutraire

Alice et Bob peuvent s'échanger un paquet de manière sécurisée sans se rencontrer.

Comment ? :

1. Alice met un message dans un coffre, le ferme avec une de ses clés et l'envoie à Bob. Ni le facteur, ni Bob ne peut ouvrir le coffre.
2. Bob met un cadenas sur le coffre, et renvoie le coffre à Alice. Le facteur ne peut toujours pas ouvrir le coffre
3. Alice enlève son cadenas et envoie le coffre à Bob. Le facteur ne peut toujours pas ouvrir !
4. Bob enlève son cadenas et peut lire le message d'Alice

La clé publique de Bob peut être comparée à un cadenas : S'il le donne ouvert à Alice, elle peut le fermer, mais ne peut pas le rouvrir. Seul Bob le peut, grâce à sa clé privée.

Fonction à sense unique

La fonction

$$f(x) = y$$

est à sens unique si :

- Étant donné x, il est facile de calculer $f(x)$
- Étant donné y, il est impossible en un *temps humainement raisonnable* de retrouver x

De bonnes fonctions à sens unique sont des fonctions telles que retrouver x à partir de $f(x)$ est un problème mathématique réputé diffcile

Exemple de fonction à sens unique

- Non-mathématiques
  - Faire le café
  - Trouver à partir d'un nom, le numéro correspondant dans un annuaire
- Mathématique
  - Exponentiation modulaire

Exponentiation modulaire

Corps : $\mathbb{Z}/p\mathbb{Z}$ est un corps ssi p est premier

Si p est premier :

- $\mathbb{Z}/p\mathbb{Z}^*$ est un groupe multiplicatif cyclique
- il existe au moin un élément g de $\mathbb{Z}/p\mathbb{Z}^*$, appelé *élément générateur* tel que :

$$\mathbb{Z}/p\mathbb{Z}^* = \{g^0, g^1, \ldots, g^{p-2}\}$$

Exemple : si $p = 13$:

- 2 est un élément générateur

$$\{2^0, 2^1, 2^2, \ldots, 2^{11}\} = \{1, 2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7\}$$

- 11 est un élément générateur

$$\{11^0, 11^1, 11^2, \ldots, 11^{11}\} = \{1, 11, 4, 5, 3, 7, 12, 2, 9, 8, 10, 6\}$$

Intérêt

Soit p un entier premier et g un générateur de $\mathbb{Z}/p\mathbb{Z}$. La fonction :

$$f : \{0, 1, \ldots, p-2\} \to \{1, 2, \ldots, p-1\}$$

$$x \mapsto g^x \mod p$$

est

- bijective (propriété indispensable pour *inverser* la fonction à sens unique)
- une fonction à sens unique bijective

pour $p = 13$ et $g = 2$ on a :

x	0	1	2	3	4	5	6	7	8	9	10	11
$f(x) = 2^x \mod p$	1	2	4	8	3	6	12	11	9	5	10	7

et pour $p = 13$ et $g = 11$ on a :

x	0	1	2	3	4	5	6	7	8	9	10	11
$f(x) = 11^x \mod p$	1	11	4	5	3	7	12	2	9	8	10	6

Calcul de l'exponentielle modulaire

- **Méthode naïve**

$u := 1$;
for $i := 1$ to x do
    $u := u * g \mod p$;

Exemple

$$u = g * g * \ldots * g$$

- **Méthode performante**

procedure expo(g, x)
if $x = 0$
then return 1
else u :=expo(g, $\lfloor x \rfloor$);
$u := u * u \mod p$;
if x est pair
then return u;
else return $g * u \mod p$;
end procedure

Exemple

$$g^{25} = g \times (((g \times g^2)^2)^2)^2$$

Problème du logarithme discret

Étant donné, $y \in \mathbb{Z}/p\mathbb{Z}$ trouver x tel que

$$g^x \mod p = y$$

est appelé problème du *logarithme discret*.

Exemples Trover x tel que

- $11^x \mod 13 = 4$
- $2^x \mod 13 = 3$

Application : protocole d'échange de clé de Diffie-Hellman (1976)

Soit p un entier premier d'au moins 230 chiffres (768 bits) et g un générateur de $\mathbb{Z}/p\mathbb{Z}$

- p et g sont publiques
- Alice :
  - Choisit $a \in \mathbb{Z}/p\mathbb{Z}$ (qu'elle garde secret)
  - Calcule $A = g^a \mod p$
  - Envoie A à Bob
- Bob :
  - Choisit $b \in \mathbb{Z}/p\mathbb{Z}$ (qu'il garde secret)
  - Calcule $B = g^b \mod p$
  - Envoie B à Alice
- Alice :
  - Reçoit B de Bob
  - Calcul $K = B^a \mod p$
- Bob :
  - Reçoit A de Alice
  - Calcul $K = A^b \mod p$

Bilan :

- $$K = A^b = B^a = (g^a)^b = (g^b)^a$$
- Paramètres publiques : p et g
- Paramètres secrets : a (connu uniquement d'Alice) et b (connu uniquement de Bob) et K le secret commun partagé par Alice et Bob.
- K le secret commun partagé par Alice et Bob

Sécurité de l'échange de clé de Diffie-Hellman

- Un attaquant veut trouver $K = g^{a \times b} \mod p$
- Problème de Diffie-Hellman : Étant donné
  - un nombre premier p et un générateur g de $\mathbb{Z}/p\mathbb{Z}$
  - $A = g^a \mod p$ et $B = g^b \mod p$
  - peut-on calculer $K = g^{a \times b} \mod p$?
- Problème ouvert : Peut-on résoudre le problème de Diffie-Hellman sans résoudre celui du logarithme discret modulo p ?

Utilisation du protocole de Diffie-Hellman

- Protocole de partage d'un secret commun à distance $\neq$ Protocole de chiffrement !
- Secret commun = clé secrète d'un algorithme de chiffrement symétrique (DES, AES par exemple)
- Puis chiffrement classique du message à envoyer.
- Diffie-Hellman : methode ne permet pas de chiffrer... mais pensent que c'est possible

Chiffrement à clé publique

- Diffie-Hellman : Chaque utilisateur à un couple de clé
  - Une clé publique (disponible dans un annuaire par exemple)
  - Une clé privée (gardée soigneusement secrète)
- Chiffrement à clé publique : principe en deux temps :
  1. Alice utilise la clé publique de Bob pour chiffrer son message.
  2. Bob utilise sa clé privée pour déchiffrer le message d'Alice
- Protocole disymétrique !
- Tout le monde peut envoyer des messages à Bob
- Mais seul Bob peut lire ses messages

Analogie

Clé secrète = Coffre fort Alice et Bob ont la clé du coffre

1. Alice utilise la clé pour déposer un message dans le coffre
2. Bob utilise la clé du coffre pour récupérer le message d'Alice

Propriétés

- Seuls Alice et Bob peuvent déposer du courrier dans le coffre
- Seuls Alice et Bob peuvent récupérer du courrier dans le coffre

Clé publique = Boîte aux lettres Seul Bob à la cléde sa boîte aux lettres

1. Alice cherche l'adresse de Bob dans un annuaire et dépose un courrier dans la boîte de Bob
2. Bob utilise sa clé secrète pour ouvrir sa boîte aux lettres

Propriétés :

1. Toute personne peut envoyer du courrier à Bob
2. Seul Bob peut récupérer son courrier

Fonction à sens unique avec trappe

Une fonction f est dite à sens unique avec trappe si :

- Étant donné x il est facile de calculer $f(x)$
- Étant donné $f(x)$, il est très difficile de retrouver x, sauf si on connait une trappe t

Diffie et Hellman n'avaient pas trouvé d'exemple de telles fonctions

Exemple de fonction à sens unique avec trappe (trouvé par Rivest, Shamir, Adleman (RSA)

La fonction puissance

Soit donné :

- p et q deux entier premier
- $n = p \times q$
- e un entier inferieur à $(p-1) \times (q-1)$.

La fonction

$$f : \{0, 1, \ldots, n-1\} \to \{0, 1, \ldots, n-1\}$$

$$x \mapsto x^e$$

est une fonction une fonction à sens unique avec trappe

Exemple

- $p = 3$ et $q = 5$ deux entier premier
- $n = p \times q = 15$
- $e = 3$ un entier inferieur à $n = 15$ et premier avec $(p-1) \times (q-1) = 8$.

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$f(x) = x^3 \mod 15$	0	1	8	12	4	5	6	13	2	9	10	11	3	7	14

- Le calcul de $f = x^e$ est linéaire en la taille de n
- L'inversion est très difficile ...
- ...Sauf si on connaît la trappe

Inversion de la fonction puissance

Objectif : inverser la fonction puissance, c'est à dire trouver des racines modulo $n = p \cdot q$

Enoncé du probleme :

Soit :

- p et q deux nombres premiers et $n = p \cdot q$
- $e \in \{1, 2, \ldots n-1\}$, premier avec $(p-1) \cdot (q-1)$
- $y \in \{1, 2, \ldots n-1\}$

Trouver $x \in \{1, 2, \ldots n-1\}$ tel que $y = x^e \mod n$

Solution :

- Si on connaît p et q c'est facile en un temps polynomial en la taille de n
- Sinon, il est difficile

Principe :

- Trouver $d \in \{1, 2, \ldots n-1\}$ tel que $e \cdot d = 1 \mod (p-1) \cdot (q-1)$
- facile
  - Si on connaît p et q
  - avec un peu de maths
- $y^d \mod n = (x^e)^d \mod n = x$

Exemple Bob doit recevoir un message de Alice

- Bob
  - choisit $p = 3$ et $q = 5$ deux nombres premiers et $n = p \cdot q = 15$
  - choisit $e = 3$, premier avec $(p-1) \cdot (q-1) = 8$
  - calcule d, la clé secréte tel que

$$e \cdot d = 1 \mod (p-1) \cdot (q-1)$$

  - il publie la clé publique : $(e, n) = (3, 15)$
- Alice veut envoyer $x = 7$ à Bob. Elle envoie

$$y = x^e \mod n = 7^3 \mod 15 = 13$$

- Bob calcule

$$y^d \mod n = 13^3 \mod 15 = 7$$

Et lorsque p et q ne sont pas connus ?

- Méthode la plus efficace connue à ce jour : Chercher d tel que
$$e \cdot d = 1 \mod (p-1) \cdot (q-1)$$
- Cela revient à trouver les deux facteurs premiers de n, p et q.
- La fonction puissance est à sens unique avec trappe s'il est difficile de factoriser n

Records

114 381 625 757 888 867 669 235 779 976 146 612 010 218 296 721 242 362 562 561 842 935 706 935 245 733 897 830 597 123 563 958 705 058 989 075 147 599 290 026 879 543 541 est le produit de deux nombres premiers, lesquels ?

- Réponse en 1995 (Atkins, Graff, Lenstra, Leyland) 8 mois de calcul fait par 600 volontaires dans 20 pays et 45 heures sur une machine massivement parallèle.
- 1er nombre premier 3 490 529 510 847 650 949 147 849 619 903 898 133 417 764 638 493 387 843 990 820 577
- 2ème nombre premier 32 769 132 993 266 709 549 961 988 190 834 461 413 177 642 967 992 942 539 798 288 533

Le chiffrement RSA (Rivest, Shamir, Adleman - 1978)

- Bob choisit deux nombres premiers p et q et un entier e premier avec $(p-1)\cdot(q-1)$.
- Il calcule $n = p \cdot q$ et d tel que $e \cdot d \mod (p-1)(q-1) = 1$
- Bob publie sa clé publique (e, n) et garde secret la clé privée d

- Alice récupère la clé publique de Bob
- Elle chiffre son message m : $C = m^e \mod n$ et l'envoie à Bob.
- Bob reçoit C et calcule $C^d \mod n$ à l'aide de sa clé secrète.
- Il retrouve ainsi m

Un attaquant veut trouver m à partir de C, autrement dit calculer une racine e-ième modulo n ce qui est aussi difficile que de factoriser n.

Exemple :

Alice

- engendre $p = 3$ et $q = 7$
- calcule $n = p \cdot q = 21$
- calcule $(p-1) \cdot (q-1) = 12$
- engendre $e = 5$
- calcule la clé secrète $d = 5$

$$e \cdot d = 1 \mod (p-1) \cdot (q-1)$$

- publie $(n, e) = (21, 5)$

Alice

- garde la clé secrète $d = 5$

Bob

- veut chiffrer la lettre B
- convertit B en 02
- demande la clé d'Alice e
- chiffre le message en calculant $y = 2^5 = 32 = 11 \mod 21$
- envoie y à Alice

Alice

- déchiffre y en calculant $y^d = 11^5 = 2 \mod 21$

Systèmes de chiffrement hybrides

- Chiffrement symétrique : gestion lourde mais rapidité de chiffrement
- Chiffrement asymétrique : gestion facile mais très lent en pratique : chiffrement hybride

- Chiffrement RSA d'un message de petite taille (la clé d'un système de chiffrement symétrique)
- Chiffrement symétrique de données de taille importante avec la clé échangée

Les différentes classes d'attaques non-conventionnel

Les méthodes d'attaques non-conventionnels des algorithmes de cryptage sont classées en trois grandes catégories selon qu'elles sont invasives ou non et selon les moyens nécessaires à mettre en oeuvre.

- Les attaques par canaux auxiliaires reposent sur l'analyse du temps d'exécution, de la consommation électrique, des émissions électromagnétiques ou des émissions acoustiques.
- Les attaques par fautes consistent à induire volontairement des erreurs dans le système pour obtenir des renseignements, par exemple en perturbant l'horloge ou l'alimentatîon, ou bien encore en modifiant quelques portes logiques du processeur à l'aide d'une décharge électromagnétique ou d'un laser.

Trouver un code PIN en 1985

Étant donné la carte à puce, il suffisait d'essayer un premier chiffre du code PIN, de déterminer, avec un oscilloscope, la durée du calcul de vérification effectué par la carte et de stopper à temps l'alimentation de la puce afin d'éviter l'enregistrement d'une tentative erronée dans la mémoire de la carte.

Vu l'implantation de l'époque, quand le chiffre était juste, le temps de calcul était moins long que quand il était faux. Par essais successifs, on déterminait ainsi le premier chiffre, puis chacun des suivants selon la même méthode

L'affaire Humpich

En 1997, Serge Humpich, ingénieur autodidacte de la puce, réussit à casser la signature RSA, alors statique et stockée dans la carte, notamment à l'aide du processus décrit page 74. Il réalisa ensuite des cartes trompant les terminaux de la RATP (les yescards) qui n'exigeaient pas une identification forte, car traitant des transactions d'un faible montant. Il tenta de monnayer son savoir-faire, mais se fit interpeller dans le cadre de la loi Godfrain. Son procès en 2000 suscita quelque effroi, car lui et ses soutiens étaient en mesure de compromettre la clé RSA en la diffusant.

- Les attaques par sondage sont des attaques invasives (destruction du circuit) qui nécessitent de gros moyens. Dans une attaque par sondage typique, il faut préparer le processeur à analyser, en le trempant dans l'acétone, puis en grattant la surface pour mettre à nu les couches supérieures du métal. On peut ensuite placer une petite pointe métallique qui réagit au passage d'un bit (microsondage du circuit). On peut aussi modifier le circuit à des endroits précis à l'aide d'une sonde ionique localisée. Quand on a ainsi percé les secrets du circuit, on peut le reproduire par rétroconception.

Sécurisation et législation

Un des problèmes rencontrés pour sécuriser la carte a été la législation française, car les moyens cryptologiques, classés dans la catégorie des armes de guerre, étaient soumis au régime défini par le décret de 1939. Ainsi, lors d'une réunion du Directoire de la cryptologie, vers 1985, le représentant du ministère de l'Industrie, en entrant à Matignon, s'excusa d'avoir pénétré dans ce lieu en portant une arme de deuxième catégorie: sa carte bancaire... Celle-ci contenait en effet un algorithme cryptographique qui interdisait sa possession.

Erosion des cryptosystèmes

la puissance des ordinateurs double tous les dix-huit mois

Erosion des cryptosystèmes

la puissance des ordinateurs double tous les dix-huit mois

Si $p \sim 2^n$ alors, pour $g, x \in \{1, 2, \ldots p-1\}$

- calculer $y = g^x$ nécessite $\sim \log_2 x \sim \log_2 p = n$ opérations
- calculer $x = \log_g y$ nécessite $\sim p = 2^n$ opérations

1er janvier 2020 : 10^8 opérations/seconde : $n = 100$, $p \sim 2^{100}$

1er janvier 2020 : 10^8 opérations/seconde : $n = 100$, $p \sim 2^{100}$

- chiffrement
  - nombre d'opérations : n
  - temps : $\frac{n}{10^8} = \frac{100}{10^8} = \frac{1}{10^6} = 1$ micro secondes

1er janvier 2020 : 10^8 opérations/seconde : $n = 100$, $p \sim 2^{100}$

- chiffrement
  - nombre d'opérations : n
  - temps : $\frac{n}{10^8} = \frac{100}{10^8} = \frac{1}{10^6} = 1$ micro secondes
- decryptage
  - nombre d'opérations : 2^n
  - temps : $\frac{p}{10^8} = \frac{2^{100}}{10^8} \sim 10^{22}$ secondes $\sim 13 \cdot 10^9 \cdot 10^3$ années

1er janvier 2020 : 10^8 opérations/seconde : $n = 100$, $p \sim 2^{100}$

- chiffrement
  - nombre d'opérations : n
  - temps : $\frac{n}{10^8} = \frac{100}{10^8} = \frac{1}{10^6} = 1$ micro secondes
- decryptage
  - nombre d'opérations : 2^n
  - temps : $\frac{p}{10^8} = \frac{2^{100}}{10^8} \sim 10^{22}$ secondes $\sim 13 \cdot 10^9 \cdot 10^3$ années

1er juin 2021 : $2 \cdot 10^8$ operations/seconde : $n = 101$, $p \sim 2^{101}$

1er janvier 2020 : 10^8 opérations/seconde : $n = 100$, $p \sim 2^{100}$

- chiffrement
  - nombre d'opérations : n
  - temps : $\frac{n}{10^8} = \frac{100}{10^8} = \frac{1}{10^6} = 1$ micro secondes
- decryptage
  - nombre d'opérations : 2^n
  - temps : $\frac{p}{10^8} = \frac{2^{100}}{10^8} \sim 10^{22}$ secondes $\sim 13 \cdot 10^9 \cdot 10^3$ années

1er juin 2021 : $2 \cdot 10^8$ operations/seconde : $n = 101$, $p \sim 2^{101}$

- chiffrement
  - nombre d'opérations : n
  - temps : $\frac{n}{2 \cdot 10^8} = \frac{101}{2 \cdot 10^8} = 0,505$ micro secondes secondes

1er janvier 2020 : 10^8 opérations/seconde : $n = 100$, $p \sim 2^{100}$

- chiffrement
  - nombre d'opérations : n
  - temps : $\frac{n}{10^8} = \frac{100}{10^8} = \frac{1}{10^6} = 1$ micro secondes
- decryptage
  - nombre d'opérations : 2^n
  - temps : $\frac{p}{10^8} = \frac{2^{100}}{10^8} \sim 10^{22}$ secondes $\sim 13 \cdot 10^9 \cdot 10^3$ années

1er juin 2021 : $2 \cdot 10^8$ operations/seconde : $n = 101$, $p \sim 2^{101}$

- chiffrement
  - nombre d'opérations : n
  - temps : $\frac{n}{2 \cdot 10^8} = \frac{101}{2 \cdot 10^8} = 0,505$ micro secondes secondes
- decryptage
  - nombre d'opérations : p
  - temps : $\frac{p}{2 \cdot 10^8} = \frac{2^{101}}{2 \cdot 10^8} \sim 10^{22}$ secondes $\sim 13 \cdot 10^9 \cdot 10^3$ années