Information, Calcul et Communication - EPFL - GC+MX - Semestre d'automne 2019-2020

Série 13

1 Chiffrement DES-X

Comme vu au cours, un moyen "simple" pour un espion de déchiffrer un message chiffré avec l'algorithme DES est l'attaque par force brute, qui consiste à essayer toutes les clés possibles (et qui est réalisable en un temps raisonnable avec les moyens informatiques dont on dipose aujourd'hui). Une amélioration de l'algorithme DES est l'algorithme DES-X, dont le principe est le suivant: pour chiffrer un message de M de 64 bits, on utilise la clé d'origine K d'une longueur de 56 bits (+ 8 bits de parité), ainsi que deux clés additionnelles K_1 et K_2, longues chacune de 64 bits (et connues également de la personne avec qui on désire communiquer). Le chiffrement est ensuite effectué de la manière suivante:

$$M' = M \oplus K_1, \quad C' = \mathrm{DES}(K, M'), \quad C = C' \oplus K_2$$

où $\mathrm{DES}(\cdot, \cdot)$ désigne le résultat du chiffrement DES esquissé au cours et C est donc le message chiffré que l'on envoie.

Sachant que 26 heures sont nécessaires actuellement pour trouver la clé d'un chiffrement DES par une attaque par force brute, combien d'heures seraient nécessaires pour trouver les clés d'un chiffrement DES-X par la même attaque par force brute?

Note: A cause de sa vulnérabilité, le système de chiffrement DES n'est plus beaucoup utilisé actuellement, mais son "grand frère", le système AES (Advanced Encryption Standard) utilise notamment le principe ci-dessus pour améliorer la confidentialité des transmissions.

2 Protocole d'échange de clé de Diffie-Hellman avec 3 personnes

Au cours, nous avons vu comment 2 personnes peuvent parvenir à se mettre d'accord sur une clé secrète K en communiquant uniquement sur un canal public, si on fait l'hypothèse que *l'exponentiation modulo P (avec P un grand nombre premier) est une opération à sens unique*, ce qui veut dire la chose suivante:

> "Même en connaissant les valeurs de P et N_1, N_3 (compris entre 1 et $P-1$) satisfaisant la relation $N_1^{N_2} \pmod P = N_3$, il est très difficile de retrouver la valeur de N_2."

Dans cet exercice, on vous propose de réfléchir à un protocole similaire permettant à 3 personnes de se mettre d'accord sur une clé secrète commune K, tout en ne communiquant que sur un canal public.

3 Chiffrement d'El Gamal (1984)

Cette méthode de chiffrement est une une version légèrement différente du protocole de Diffie-Hellman, qui permet de directement envoyer un message lors du chiffrement:

- A choisit tout d'abord un grand nombre premier P, ainsi que deux nombres entiers Q et N_1 compris entre 1 et $P-1$; il calcule ensuite $N_2 = Q^{N_1} \pmod P$, et publie P, Q et N_2.

- Pour communiquer un message M à A (on supposera ici que le message M peut être représenté par un nombre entre 1 et $P-1$), B tire au hasard un nombre R entre 1 et $P-1$ et envoie à A le message crypté suivant, composé de deux parties: $(Q^R \pmod P, M \cdot N_2^R \pmod P)$.

- Pour déchiffrer le message envoyé par B, que fait A? A vous de jouer!

- Et si quelqu'un d'autre que A intercepte le message de B, peut-il le déchiffrer?

4 Pour le plaisir: trouver un grand nombre premier*

Comment faire pour trouver un grand nombre premier efficacement? C'est une étape nécessaire dans l'implémentation du protocole de Diffie-Hellman! Depuis Euclide, on sait qu'il existe une infinité de nombres premiers et aussi que ceux-ci ont tendance à se raréfier parmi les grands nombres. Le *théorème des nombres premiers* (établi en 1896) dit plus précisément que $\pi(X)$, le nombre de nombres premiers plus petits ou égaux à un nombre entier donné X, est donné approximativement par

$$\pi(X) \simeq \frac{X}{\log(X)}$$

a) Supposons qu'on tire au hasard un nombre entier N à n chiffres (i.e., un nombre choisi uniformément entre 10^{n-1} et $10^n - 1$). En se basant sur la relation ci-dessus, pouvez-vous déduire approximativement quelle la probabilité que N soit un nombre premier?

Comment faire maintenant pour décider si N est un nombre premier? On pourrait bien sûr appliquer l'algorithme vu dans la première partie du cours, i.e., tester si N est divisible par un autre nombre premier P compris entre 2 et $\sqrt{N}$, mais ceci prendrait de l'ordre de $10^{n/2}$ opérations, ce qui n'est pas faisable en pratique pour de grandes valeurs de n.

b) Ceci dit, sans aller jusqu'à $\sqrt{N}$, on peut déjà très facilement tester si N est un multiple de 2, 3 ou 5, par exemple, ce qui nous permet de nous débarasser rapidement d'un grand nombre de cas. Quelle est la proportion de ces nombres parmi tous les nombres qu'on tire au hasard?

Supposons maintenant que N ne rentre pas dans la catégorie ci-dessus. Pour tester si N est un nombre premier, on utilise le théorème suivant, appelé *petit théorème de Fermat*:

> Si P est un nombre premier, alors $Q^{P-1} (\text{mod } P) = 1$ pour tout nombre entier Q compris entre 1 et $P - 1$.

Basé sur ce théorème, vous choisissez un nombre Q au hasard entre 1 et $N - 1$, et calculez $X = Q^{N-1} (\text{mod } N)$.

c) Que pouvez-vous conclure si le résultat X vaut 1? Et si le résultat X est différent de 1?

Pour aller plus loin dans le raisonnement, on utilise cet autre résultat, qui dit que

> S'il existe Q compris entre 1 et $N - 1$ tel que $\text{pgcd}(Q, N) = 1$ et $Q^{N-1} (\text{mod } N) \neq 1$,
> alors c'est aussi vrai pour au moins la moitié des autres valeurs de Q entre 1 et $N - 1$.

Vous tirez maintenant k nombres $Q_1, Q_2, \ldots, Q_k$ au hasard entre 1 et $N - 1$ et calculez

$$X_1 = Q_1^{N-1} (\text{mod } N), \quad X_2 = Q_2^{N-1} (\text{mod } N) \quad \ldots \quad X_k = Q_k^{N-1} (\text{mod } N)$$

d) Que pouvez-vous conclure si $X_1 = X_2 = \ldots = X_k = 1$? Et s'il existe $1 \leq j \leq k$ tel que $X_j \neq 1$?

e*) Pouvez-vous estimer l'ordre de grandeur du nombre d'opérations effectuées pour trouver un nombre premier à n chiffres en suivant la procédure ci-dessus?