EPFL - Information, Calcul et Communication - Partie théorique

Série 13

1 Chiffrer et déchiffrer

a) Pour chiffrer un message composé de lettres majuscules de A à Z, on utilise le système de substitution suivant. A chaque lettre de l'alphabet, on fait correspondre une autre lettre, par exemple:

$$A \to K, \quad B \to H, \quad C \to D, \quad D \to F, \quad E \to A, \quad F \to P, \quad \text{etc.}$$

On suppose ici que chaque lettre est utilisée une et une seule fois, i.e., qu'il y a une correspondance univoque entre l'alphabet d'origine et celui utilisé pour le chiffrement.

Une attaque par force brute de ce système permet de déchiffrer un message en une heure en testant toutes les substitutions possibles. Combien d'heures cette même attaque nécessitera-t-elle pour déchiffrer un message écrit avec un alphabet de 28 lettres et chiffré avec la même méthode?

b) Supposons qu'une clé K d'une longueur de 20 bits soit utilisée pour chiffrer un message binaire d'une longueur sensiblement plus grande (on ne spécifie pas ici le système de chiffrement utilisé). Supposons également qu'avec une attaque par force brute avec un ordinateur donné, il soit possible de trouver la clé K (et donc de déchiffrer le message) en 5 minutes. Si maintenant une clé K' deux fois plus longue est utilisée pour chiffrer le message, combien de temps sera nécessaire pour déchiffrer le message avec une même attaque par force brute, si on dispose d'un ordinateur cent fois plus puissant que le premier (i.e., un ordinateur effectuant cent fois plus d'opérations par seconde)?

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 $N_1^{N_2} (\text{mod } P) = N_3$, 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 $N_2 = Q^{N_1} (\text{mod } P)$, 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: $(Q^R (\text{mod } P), M \cdot N_2^R (\text{mod } P))$.

- 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 $Q^{P-1} \pmod{P} = 1$ 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 $X = Q^{N-1} \pmod{N}$.

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 $\mathrm{pgcd}(Q, N) = 1$ et $Q^{N-1} \pmod{N} \neq 1$,
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

$$X_1 = Q_1^{N-1} \pmod{N}, \quad X_2 = Q_2^{N-1} \pmod{N} \quad \ldots \quad X_k = Q_k^{N-1} \pmod{N}$$

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?