Chiffrement et clef de chiffrement

Chiffrer consiste à mélanger de façon plus ou moins inextricable les informations élémentaires d'un texte (lettres, chiffres, bits…). Le chiffre employé par Jules César dans ses correspondances secrètes fournit un exemple simpliste de chiffrement : César se contentait de décaler l'alphabet latin de trois lettres. Son propre nom, CESAR, devenait ainsi FHVDU. Le chiffre de César peut être étendu aux 26 décalages alphabétiques possibles, ce qui explique que des appareils à chiffrer ainsi aient été vendus aux commerçants et aux militaires jusqu'au XIXe siècle *(ci-dessous)*. Il peut aussi être généralisé aux chiffrements polyalphabétiques, qui consistent à substituer les lettres de l'alphabet par d'autres tirées du même alphabet, voire d'un autre. Pendant sa captivité, la reine Marie-Antoinette employa ce type de chiffre *(ci-dessus, l'une de ses lettres)*.

Tout chiffrement implique un algorithme de déchiffrement. Dans le cas du chiffre de César, il suffit de décaler l'alphabet de trois lettres dans le sens opposé pour déchiffrer.

Dans la pratique cryptologique, l'algorithme de (dé)chiffrement est public, de sorte que la sécurité réside dans la clef qui spécifie le chiffrement effectué. Cette clef est le nombre 3 dans le cas du chiffre de César, ce qui est bien trop simple pour résister à des essais de déchiffrement systématiques (la force brute). Pour produire une clef plus difficile à découvrir, on pourra par exemple décaler de 3 lettres la première phrase, de 1 lettre la deuxième, de 4 la troisième, puis de 1, de 5, de 9, de 2, de 6, de 5,… et nommer π la clef résultante. Mais cela serait encore bien trop simple !

Jacques Patarin et Valérie Nachef

Après la robustesse, le deuxième critère à prendre en compte dans le choix d'une primitive cryptographique est la facilité avec laquelle on pourra la mettre en œuvre dans la situation à traiter. Si placer dans un appartement ou une maison particulière un coffre-fort aux parois d'acier de dix centimètres d'épaisseur et pesant cinq tonnes semble une précaution exagérée, ce n'est pas le cas dans une banque. De même, les contraintes qui accompagnent l'emploi d'une primitive cryptographique restreignent ses applications.

Les systèmes de sécurisation des données embarqués dans un téléphone portable, par exemple, sont limités en mémoire et en puissance de calcul, ce qui y interdit les primitives trop complexes ; la situation est différente si les données à protéger ont vocation à être stockées sur un serveur.

Une fois la primitive choisie, il reste à fixer la taille de la clef de chiffrement à utiliser. Une telle clef consiste en une série de bits (de valeurs 0 ou 1) déterminant la façon dont s'opère le cryptage avec un algorithme donné. Dans le cas des algorithmes dits symétriques, la clef spécifie aussi le déchiffrement. Dans celui des algorithmes dits asymétriques, elle ne sert qu'au chiffrement, et une clef supplémentaire est nécessaire au déchiffrement. Quoi qu'il en soit, un principe général prévaut : plus une clef est longue, plus il sera difficile de casser le chiffrement correspondant et le cryptosystème dont elle est le cœur.

L'ESSENTIEL

- Les données stockées ou circulant en masse sur Internet sont protégées par des systèmes de sécurité.
- Les attaques peuvent porter soit sur leur couche cryptographique, soit sur leur couche logique.
- La solidité de la première dépend de la longueur de la clef de chiffrement ; celle de la seconde, des détails de la mise en œuvre du système.
- Les attaquants tentent aussi d'exploiter toute fuite involontaire d'information que présente le système.

Hubert Berberich

Attaques par force brute

Ce principe général s'explique facilement si l'on considère le cas d'un algorithme symétrique public – c'est-à-dire connu et employé par qui veut. Supposons ce mode de cryptage contrôlé par une clef comportant N bits. Pour le casser, il existe toujours, en dernier ressort, la méthode dite de la force brute : elle consiste tout simplement à essayer, avec l'aide d'un ordinateur, toutes les clefs possibles, soit 2^N clefs. Dans le cas d'une clef de 320 bits, on aura donc $2^{320} \simeq 2 \times 10^{96}$ clefs (plus que d'atomes dans l'Univers…) à tester. Face à de tels nombres, la méthode de la force brute paraît bien illusoire. Mais la prudence s'impose : avec l'augmentation incessante de la puissance de calcul des superordinateurs massivement parallèles (à très nombreux processeurs calculant en même temps), l'expérience a montré que l'on a pu casser des primitives d'usage courant, dont les clefs étaient considérées jusque-là comme assez longues pour être sûres…

L'algorithme de cryptage AES *(Advanced Encryption Standard)*, par exemple, s'emploie aujourd'hui avec des clefs de 128, 192 ou 256 bits. Cet algorithme fait subir aux blocs successifs de données un triturage numérique complexe comprenant des permutations, des rotations dans un espace mathématique abstrait, etc., le tout répété plusieurs fois selon la longueur de la clef. En 2011, Christian Rechberger, de l'Université technique de Copenhague, et deux collègues ont publié une méthode d'attaque d'AES-128 (avec clef de 128 bits) environ quatre fois plus rapide que la force brute. Son déroulement implique à peu près 2^{126} (environ 10^{38}) opérations pour trouver la clef. Un ordinateur effectuant dix milliards d'opérations par seconde mettrait de l'ordre de 3×10^{20} années pour faire le calcul, soit plusieurs milliards de fois l'âge de l'Univers : on comprend qu'AES-128 soit encore considéré comme sûr…

Ce cas illustre que plus la clef d'un algorithme est longue, plus il faut de temps