Crypto, Sécurité, Réseaux

TD 1

## La transmission sécurisée des messages : le chiffre de César

La transmission sécurisée des messages a toujours représenté un défi important dans notre société. Nous pouvons par exemple penser à des applications militaires ou juste dans le contexte de la protection des informations sensibles.

C'est pourquoi nous utilisons le **chiffrement** pour cacher le contenu des messages transmis entre deux parties. Le chiffrement garantit notamment la **confidentialité** des messages chiffrés. La forme la plus simple de chiffrement c'est la méthode de César (appelée ainsi car elle est supposé avoir été utilisé par Jules César). La méthode consiste a permuter les lettres de l'alphabet par une constante (3 dans le cas du chiffré César classique). Donc A devient D, B devient E, M devient P, Z devient C etc.

- Faites un tableau avec deux lignes. Sur la première ligne listez les lettres de l'alphabet (la version anglaise à 26 lettres, sans accents et lettres spéciales comme œ, é, û, etc.). Sur la deuxième ligne écrivez la permutation par 3 lettres du même alphabet.

- Utilisez votre tableau et le chiffre César pour chiffrer le message suivant :

  CECIESTMONPREMIERCHIFFREMENTCESAR

- Généralisez votre tableau pour inclure 26 lignes. Sur la première ligne vous aurez toujours l'alphabet à 26 caractères. Sur la deuxième, la permutation de cet alphabet par une lettre. Sur la troisième, une permutation par deux lettres. Vous continuerez ainsi jusqu'à la dernière ligne, sur laquelle vous aurez la permutation par 25 lettres.

- Le chiffré prochain est obtenu par un chiffrement généralisé César, c'est-à-dire une permutation par k lettres, avec k inconnu et $0 < k < 26$ . Répondez à la question chiffrée.

  YNPYRSQRPRPUVSSERZRAGRFGGERVMRIENVBHSNHK

L'attaque mise en place pour résoudre cette dernière question s'appelle une attaque par force brute (en anglais « brute force attack ») : nous devons essayer toutes les possibilités pour trouver le message secret.

Une alternative à une cryptanalyse par force brute est d'utiliser des statistiques caractérisant une langue (par exemple une analyse de la fréquence des lettres) et/ou des connaissances a priori sur une partie du message chiffré (par exemple le fait que le message contient le mot « cordialement »).

# Le chiffrement à clé symétrique et le chiffré de Vigenère

Le chiffrement de César est un exemple d'une technique plus générique, le chiffrement à clé symétrique. Un schéma de chiffrement est symétrique lorsque la même clé est utilisée pour chiffrer un message et pour déchiffrer un chiffré. Toutefois, l'algorithme de chiffrement peut être très différent de l'algorithme de déchiffrement.

Dans le cas du chiffrement de César, la clé est un entier entre 0 et 26. Une forme de chiffrement plus avancée est celle de Vigenère. Dans cette méthode la clé sera un mot ou une phrase d'une taille fixe (par exemple le mot « CLEF »). Pour chiffrer un message, disons le message « MESSAGE », nous allons premièrement obtenir une clé de la même longueur que le message à chiffrer (autrement dit, le texte clair), en alternant la clé un nombre de fois. Donc pour un message de 7 lettres et une clé de 4 lettres, nous obtenons la clé suivante de 7 caractères : CLEFCLE. Si le message avait, disons 10 lettres, la clé aurait été : CLEFCLEFCL.

Pour ensuite chiffrer le message MESSAGE avec la clé CLEFCLE nous allons chiffrer lettre par lettre. La première lettre du texte claire (M) sera chiffrée avec la première lettre de la clé (C). Ceci veut dire simplement permuter la lettre M par le nombre de positions correspondant à l'index, dans l'alphabet, de la lettre C. Donc M deviendra O. Puis, pour la deuxième lettre du message, il faut permuter la lettre du texte clair (E) par l'index de la deuxième lettre de la clé (L) dans l'alphabet, c'est-à-dire 11. Donc E deviendra P. Ce procédé doit se répète pour chaque lettre.

- Chiffrez le mot MESSAGE avec la clé CLEF en utilisant le chiffré de Vigènere.
- Déchiffrez le chiffré EMVZSFVCGDSFUIZVQUKNYIS avec la clé CITRON

Le chiffré de Vigènere est beaucoup plus difficile à casser en utilisant juste de la force brute. Une première étape de la cryptanalyse de Vigènere, c'est d'apprendre la longueur de la clé. Une méthode de trouver la longueur de la clé, c'est de chercher des suites identiques de 2 ou plusieurs lettres dans des positions différentes dans le chiffré. Cette méthode marchera bien si on a un chiffré beaucoup plus gros que la clé.

Nous prendrons le chiffré suivant :

AOKJQDGDUZSHVVTSALMBRSSAVAGPXDTAFSFSSTSUFLEHWDGUVTGILLOPWOVLSDEDHMYWFQTGU
WKGNVSASKGHGOVLUCAUWLWFHVPZQLWOHIVMFLWPXHMWLWAISOJAHRTBASARNCHAGMJRCHL
WKSPGSBKGIPASAWDZRHSLAKHVCUCWVSYPGBWYOADUZSHVVTECAXOVIDIKKSEXBIHWFPJIVEWGF
PUMVSBFJBIMLFRBSAKSURPZWJKEHTZIUJMCICOJSDUXSZWFRHCAMKKOTTWVLWZYXUQTDSNPIBJW
EHTECAVSQGCQL

Une caractéristique principale d'une langue, c'est la répétition de mots, par exemple « le », « la », « et »… Si dans notre chiffré ces mots sont chiffrés avec la même lettre de la clé, alors le chiffré résultant sera identique également. La distance entre les deux tuples identiques de lettres nous donnera un indice sur la longueur de la clé, notamment : cette distance devrait être un multiple de la longueur de la clé utilisée. Plus les chaines de caractères identiques seront longues, plus nous serons sûrs que la répétition n'est pas une coïncidence. Finalement nous allons deviner que la longueur de la clé est le plus grand diviseur commun de ces distances. Ce processus est la méthode de Kasiski.

Pour simplifier votre tâche vous allez partir sur l'hypothèse que la clé a une longueur au plus égale à 10 lettres.

- Trouvez des chaines de caractères identiques dans le chiffré donné et mesurez la distance entre le premier caractère de la première chaine et le premier caractère de la deuxième.
- Quelle est la longueur de la clé que vous pouvez deviner ?

Disons que la longueur de la clé est k, avec $1 < k < 11$. Cela veut dire que les lettres 1, 1+k, 1+2k, … sont un chiffré César avec la clé donnée par l'index dans l'alphabet de la première lettre de la clé. Là, nous pourrons utiliser la force brute pour essayer de deviner la clé. Nous allons faire cela pendant les TPs.

La faiblesse principale du chiffrement de Vigenère c'est la répétition, dans le texte clair et dans le chiffré. Nous ne pouvons rien faire contre les répétitions du texte clair, mais si la clé était aussi longue que le texte, cette répétition ne serait plus apparente. Le chiffré de Vernam (ou le chiffrement par masque jetable – one-time pad) utilise précisément ce principe. Il s'applique principalement au chiffrement des chaines binaires (des chaines de 1 et 0). Le chiffrement d'un texte clair (par exemple 0011010101110) par une clé (unique), par exemple 1101001101000 se fait par l'opération d'OU exclusif (Exclusive OR = XOR).

- Rappelez le fonctionnement de l'opération d'XOR.
- Quel chiffrement obtenez-vous pour le message et la clé donnés ?

Le chiffrement à masque jetable est un chiffrement parfait : il cache, statistiquement, le message chiffré, tant que la clé est choisie aléatoirement. Toutefois, il a des inconvénients.

- Quels seraient les inconvénients du chiffrement à masque jetable ?

## Le chiffrement symétrique et à clé publique

Pour le chiffrement à clé publique, les deux parties qui communiquent doivent savoir la clé avant de pouvoir commencer à communiquer.

- Disons qu'on a quatre amis : Amélie, Baptiste, Charles et Diane. Nous voulons donner la possibilité à chaque paire d'amis de communiquer de façon sécurisée. De combien de clés avons-nous besoin ?

Le chiffrement à clé publique représente une autre façon de sécuriser la communication entre deux parties. Dans ce contexte, chaque participant génère une clé privée et une clé publique (qui sont d'habitude liées l'une à l'autre). La clé publique est rendue publique, donc n'importe qui pourra utiliser cette clé ; par contre la clé privée doit être gardée précieusement. Un bon parallèle est un compte mail : l'adresse mail est publique, tandis que le mot de passe reste privé. Par contre, attention : l'échange des mails n'est pas un système de chiffrement !

Le chiffrement des messages se fait exclusivement avec la clé publique : notamment, n'importe qui peut chiffrer des messages pour un utilisateur donné (dans notre parallèle, nous pouvons envoyer des mails juste en connaissant l'adresse mail du correspondant). Par contre, le déchiffrement ne s'effectue qu'avec la clé secrète (nous ne pouvons pas lire nos mails sans le mot de passe).

Le chiffrement à clé publique est moins efficace que celui à clé symétrique. Par contre il peut avoir des avantages remarquables : on peut échanger des messages de façon sécurisée sans avoir échangé en préalable une clé symétrique, le chiffrement donne des garanties de sécurité plus fortes, et la gestion de clés est plus simple.

- Pour le cas de nos quatre amis, de combien de (paires de) clés avons-nous besoin pour assurer des communications sécurisées entre chaque paire d'amis.