Chiffres de substitution

Tout comme cela sonne, un chiffre de substitution substitue une lettre ou un caractère à un autre. Enfant, vous avez peut-être reçu un anneau décodeur secret grâce à une offre sur une boîte de céréales ou du lait en poudre au chocolat. L'anneau décodeur se composait de deux cadrans, tous deux contenant toutes les lettres de l'alphabet. L'astuce consistait à faire tournoyer un cadran autour de l'autre afin que les lettres de l'alphabet ne correspondent pas. Ensuite, vous avez trouvé la lettre que vous vouliez utiliser sur un anneau et avez remplacé la lettre sur l'autre anneau. Continuez lettre par lettre et vous avez alors un message secret. Bien qu'il ne s'agisse techniquement pas d'un anneau illustré ci-dessous, voici un exemple de la façon dont les substitutions s'aligneraient :

Bien sûr, pour déchiffrer votre message, votre destinataire devrait également avoir une sonnerie de décodeur et il aurait besoin de savoir jusqu'où tourner son cadran pour qu'il corresponde au vôtre. Ce numéro indiquerait le commutateur en lettres - et c'est aussi la clé pour décrypter le message. Dans l'exemple ci-dessus, le commutateur est à 18 lettres à droite de la lettre A ; par conséquent, la clé est "18". Ce chiffre est probablement l'un des plus connus au monde et est également appelé le « chiffre de César » en raison de références historiques liant Jules César et ce type de chiffre.

Chiffrements par transposition

L'un des plus anciens chiffrements connus est appelé chiffrement par transposition. Ce type de chiffrement modifie l'ordre des lettres du message d'origine. Une méthode consiste à écrire le message dans une série de colonnes et de lignes dans une grille - ou vous pouvez écrire le message à l'envers. L'un des plus anciens chiffrements de transposition est le scytale spartiate (également orthographié comme skytale). Cette information provient de Plutarque, qui était un ancien prêtre et érudit grec. Plutarque raconte comment les généraux lacédémoniens échangeaient des messages en enroulant en spirale un étroit ruban de parchemin autour d'un bâton ou d'une lance. Le message a ensuite été écrit dans le sens de la longueur à travers le parchemin enroulé. Lorsque le parchemin était déroulé, vous ne pouviez voir que des parties de mots ou de phrases qui étaient écrites et le motif des mots semblait aléatoire. Ce chiffre ne pouvait être lu que par la personne qui avait une lance d'exactement la même circonférence, qui pouvait rembobiner le parchemin, de sorte que les lettres réapparaissaient dans leur ordre d'origine. Si la lance utilisée était trop épaisse ou trop fine, les mots ne correspondaient pas lorsque le parchemin était enroulé autour d'elle. Ainsi, dans ce cas, le récepteur devait connaître deux secrets -- ou deux clés -- pour lire le message.

La machine de chiffrement allemande Enigma Le chiffrement par substitution le plus connu est la machine Enigma qui a été utilisée par les Allemands pendant la Seconde Guerre mondiale pour chiffrer leurs messages militaires secrets. La machine Enigma ressemblait à peu près à une machine à écrire, sauf qu'elle avait un certain nombre de rotors différents, un peu comme le compteur kilométrique de votre voiture. Ces rotors ont été placés les uns à côté des autres sur un arbre, puis tournés pour régler le décalage en lettres pour la substitution. Mais parce qu'il y avait plus d'une substitution impliquée, les messages étaient encore plus brouillés qu'en utilisant la substitution unique que j'ai utilisée dans l'exemple ci-dessus.

La machine Enigma a été l'une des premières utilisations d'un chiffrement fort. Il a fallu l'effort concerté de nombreuses nations, de nombreux esprits et un certain nombre d'années pour enfin déchiffrer le code Enigma.

Il devait savoir enrouler le parchemin autour d'une sorte de lance, et il devait aussi savoir quelle devait être l'épaisseur de la perche.

Alors que les chiffrements de substitution préservent l'ordre des lettres utilisées dans le message, les chiffrements de transposition réorganisent les lettres. Les chiffrements de transposition sont rarement utilisés de nos jours, mais ils ont été très importants dans le passé.

Bien qu'il existe littéralement des centaines de types différents, je vais vous montrer l'un des plus simples. Vous pouvez le faire vous-même, tout ce dont vous avez besoin est du papier et un crayon.

Le message crypté vous parvient comme suit :

Vous avez peut-être remarqué que le message crypté ne correspondait pas au même espacement que le message décrypté. C'est fait exprès pour (espérons-le) vous confondre davantage. Si vous ne savez pas où commence un mot et un autre, il est plus difficile pour un spectateur occasionnel de comprendre ce qui est écrit. Dans de nombreux anciens messages cryptés, vous remarquerez que les messages sont en majuscules et sont écrits en groupes de cinq lettres. En fait, il est devenu un standard de taper un message par groupes de cinq lettres pour les messages cryptés simples.

Chiffrements de dissimulation

Les chiffrements de dissimulation sont utilisés depuis des siècles pour cacher un message à la vue de tous. Ils ont été utilisés pour donner des ordres aux troupes en guerre, pour indiquer aux espions où rencontrer leurs contacts et même pour aider des personnes comme Mary, reine d'Écosse,

coordonner les rendez-vous avec ses admirateurs.

Le paragraphe suivant est un exemple d'un chiffre de dissimulation très ancien qui a été donné à un prisonnier en Angleterre à l'époque d'Oliver Cromwell. Cachées dans le message se trouvent les instructions au prisonnier sur la façon de s'évader :

Worthie Sir John: L'espoir, qui est le meilleur réconfort des affligés, ne peut pas beaucoup, je le crains, vous aider maintenant. Ce que je voudrais vous dire, c'est ceci seulement : si jamais je peux vous rendre ce que je vous dois, ne vous arrêtez pas à me demander : Je ne peux pas faire grand-chose : mais ce que je peux faire, abeille, vous êtes sûr que je le ferai. . Je sais que, si la mort vient, si les hommes ordinaires la craignent, cela ne vous effraie pas, c'est un grand honneur que d'avoir une telle récompense de votre loyauté. Priez encore pour que vous puissiez être épargné de cette coupe si amère, je ne crains pas que vous en vouliez des souffrances; seulement si la soumission vous pouvez les détourner, c'est le rôle d'un homme sage. Dites-moi, comme si vous le pouvez, je fais pour vous tout ce que vous pouvez faire. Le général repart mercredi. Restinge votre serviteur à commander. R. J.

Je ne sais pas comment la clé a été donnée au prisonnier pour qu'il puisse déchiffrer le message, mais la clé est "la troisième lettre après chaque signe de ponctuation". Si vous suivez cette clé, vous constaterez que le message caché est :

"panneau à l'extrémité est des diapositives de la chapelle" Et, oui, le prisonnier s'est échappé ! Il a demandé à se rendre à la chapelle avant son exécution afin de pouvoir prier pour son âme. Les gardes le laissèrent dans la chapelle et surveillèrent l'entrée. Quand ils ont pensé qu'il avait eu assez de temps et sont allés le voir, surprise ! Pas de prisonnier ! Comment expliquez-vous celle-là au roi ?

Clés asymétriques

Juste au moment où vous pensiez avoir trouvé toutes les clés, je vais en lancer une autre dans les travaux. Là où la section précédente se concentrait sur les clés et les algorithmes symétriques, cette section se penche sur les clés et les algorithmes asymétriques.

L'un des plus gros problèmes avec les algorithmes à clé symétrique est qu'il est difficile à la fois de partager la clé et de la protéger. Étant donné que vous utilisez la même clé pour chiffrer et déchiffrer les données, il n'y a aucun moyen de contourner le fait que vous devez partager la clé. Comme la clé de votre porte d'entrée, il est possible que quelqu'un vole la clé ou la copie.

Les clés asymétriques résolvent le problème de la distribution des clés en créant deux clés distinctes qui sont mathématiquement connectées. Vous utilisez une clé « privée » que vous ne révélez jamais à personne pour déchiffrer les données que vous avez reçues et le destinataire utilise sa clé « publique » correspondante que tout le monde peut avoir pour chiffrer les données. En fait, cette explication est un peu simpliste, mais vous voyez l'idée. Une idée similaire est un coffre-fort bancaire. La banque a une clé qu'elle garde privée et elle a une clé publique qu'elle vous donne. Lorsque vous allez déverrouiller votre coffre pour y déposer vos objets de valeur, vous avez besoin à la fois de la clé de la banque et de votre clé dans les serrures pour pouvoir ouvrir la porte du coffre.

Les clés asymétriques utilisent des nombres premiers comme point de départ. La première partie du processus consiste à créer un très grand nombre en multipliant ensemble deux très longs nombres premiers. Les nombres premiers, si vous vous souvenez de votre algèbre du secondaire, sont des nombres qui ne peuvent être divisés que par le nombre 1 ou le nombre lui-même. Un exemple de nombre premier est le nombre 7. Peu importe vos efforts, 7 ne peut être divisé que par 1 ou 7. Maintenant, disons que vous multipliez deux nombres premiers ensemble. Si vous multipliez 5 x 7, vous obtenez 35. Il n'est pas trop difficile de travailler à rebours à partir du nombre 35 pour déterminer quels deux nombres premiers ont été utilisés pour le créer. Mais, si vous utilisiez un nombre de plus de 100 chiffres, à quel point pensez-vous qu'il serait difficile de trouver les deux nombres qui ont été utilisés pour le créer ? Allez-y, prenez votre papier et votre crayon. J'attendrai.

Vous avez probablement trouvé la même réponse que moi : cela prend énormément de temps ! Même si vous traversez tous ces ennuis, vous n'avez qu'un seul numéro. Vous avez encore un long chemin à parcourir. De ce nombre long, vous en dérivez une partie (via un calcul mathématique) pour la clé privée, et de la clé privée vous en dérivez une partie pour la clé publique. L'élégance de ce processus est que vous ne pouvez pas désosser la clé publique et obtenir la clé privée.

Bien que ce concept de clé privée/publique soit considéré comme fort, vous avez besoin d'au moins une clé de 2 304 bits pour atteindre le même niveau de sécurité qu'un algorithme symétrique de 128 bits. Les algorithmes asymétriques sont lents à traiter et il n'est pas pratique de les utiliser pour chiffrer de grandes quantités de données. Les algorithmes symétriques peuvent être environ 1 000 fois plus rapides que les algorithmes asymétriques.

Par conséquent, vous voyez généralement des algorithmes asymétriques utilisés pour protéger de petites quantités de données telles que des messages électroniques et - de petits fichiers de données tels que des pièces jointes aux messages.

RSA

Il s'agit probablement de l'algorithme asymétrique le plus reconnaissable, en partie grâce à la très grande entreprise qui le soutient : RSA Data Security. RSA vient des noms de famille des inventeurs, Ron Rivest, Adi Shamir et Leonard Adleman, qui ont créé l'algorithme en 1978. À ce jour, c'est le seul algorithme asymétrique largement utilisé à des fins privées/

génération de clé publique et cryptage. Deux autres algorithmes appelés ElGamel et Rabin génèrent également deux clés et les chiffrent, mais vous ne les voyez pas utilisés aussi souvent que RSA. Étant donné que la plupart des autres algorithmes asymétriques ne génèrent que deux clés, de nombreux programmes utilisent une combinaison d'algorithmes asymétriques et d'algorithmes symétriques pour protéger les données.

RSA utilise des nombres premiers pour créer chacune des clés (privées et publiques), mais l'utilisation de ces clés pour chiffrer une grande quantité de données n'est pas pratique en raison du temps nécessaire à un ordinateur pour traiter le chiffrement. Le plus souvent, un programme de chiffrement qui utilise RSA chiffre les données avec un algorithme symétrique tel que RC4 (ou DES, ou IDEA, etc.). Ensuite, la clé symétrique créée par RC4 est chiffrée avec la clé publique du destinataire. Lorsque le destinataire reçoit le message, il utilise sa clé privée pour déchiffrer la clé RC4,

et lorsque la clé RC4 est déchiffrée, la majeure partie du message peut être déchiffrée.

Diffie-Hellman (& Merkle)

Cet algorithme est communément appelé DH, qui représente les noms de famille de deux des inventeurs. Cependant, si vous deviez rencontrer Whit Diffie ou Martin Hellman, ils ne manqueraient pas de souligner qu'ils n'auraient pas pu faire ce qu'ils ont fait sans le travail de Ralph Merkle. Ce n'est que par malchance que l'article de Diffie et Hellman est paru avant celui de Merkle, même s'ils sont tous arrivés à la même idée à peu près au même moment. Donc, par respect pour les auteurs, veuillez vous souvenir de Merkle.

Il existe une énorme différence entre RSA et DH dans la mesure où l'algorithme DH n'est pas utilisé pour le chiffrement. Hein? C'est vrai -- DH n'est pas un algorithme de cryptage ; il s'agit plutôt d'un algorithme d'échange de clés. Diffie, Hellman et Merkle étaient plus préoccupés par le problème du partage d'une clé sur un canal non sécurisé que par le cryptage des données, ils ont donc proposé une solution qui a créé un moyen de partager un secret.

Voici comment ça fonctionne:

1. Natasha possède une paire de clés DH composée d'une clé privée qu'elle garde pour elle et d'une clé publique qu'elle envoie à Boris.

2. Boris reçoit la clé publique de Natasha et utilise l'algorithme DH pour créer une clé privée temporaire et une clé publique temporaire pour lui-même. (Notez que les clés de Boris ont quelque chose en commun avec la clé publique de Natasha.) 3. Boris prend maintenant sa clé privée nouvellement créée et la clé publique de Natasha et demande à l'algorithme DH de générer un numéro secret.

4. Boris utilise le numéro secret (au lieu d'un RNG ou d'un PRNG) pour générer une clé uniquement pour cette transaction. C'est ce qu'on appelle une clé de session.

5. Boris utilise la clé de session pour chiffrer les données et les envoie à Natasha avec sa clé publique temporaire.

6. Lorsque Natasha reçoit le message crypté, elle peut dériver la clé de session car ses clés et les clés de Boris ont la même dérivée - sa clé publique.

7. Avec la clé de session retirée du message, Natasha peut maintenant déchiffrer le message.

Veuillez noter que lorsque je dis « Natasha fait ceci » et « Boris fait cela », je veux vraiment dire qu'ils utilisent leur programme de cryptage pour effectuer ces actions.

Les seules actions réelles de Natasha et Boris sont de répondre à toutes les boîtes de dialogue qui apparaissent pendant le processus. Bien sûr, le programme de cryptage contient l'algorithme d'échange de clés DH, sinon rien de tout cela ne serait possible.

Présentation de Boris et Natasha Si vous avez déjà parcouru d'autres livres grand public sur la cryptographie, vous avez probablement remarqué que l'expéditeur et le destinataire s'appellent généralement Alice et Bob. Cela s'est avéré plus facile que de dire "L'expéditeur A crypte un message à donner au destinataire B." Il existe d'autres personnages qui jouent les rôles d'intercepteur, de pirate informatique et de tiers de confiance.

J'ai décidé d'utiliser Boris et Natasha simplement pour ajouter un peu d'humour aux exemples et parce qu'ils sont parfaitement interprétés comme des personnages susceptibles d'utiliser des messages secrets. Rocky et Bullwinkle peuvent également apparaître, alors surveillez-les !

PGP

Permettez-moi de dire ceci dès le départ : PGP (Pretty Good Privacy) n'est pas un algorithme de cryptage, bien que beaucoup de gens aient tendance à le penser de cette façon. PGP est en fait un programme de chiffrement qui utilise à la fois des algorithmes symétriques et asymétriques pour chiffrer les données. Il est le plus souvent utilisé pour le courrier électronique car il possède de très bons plug-ins de programme de courrier électronique, mais il peut également être utilisé pour le chiffrement de disque et pour effacer en toute sécurité les données d'un disque.

PGP est un cryptosystème hybride. Lorsqu'un utilisateur chiffre du texte en clair avec PGP, PGP compresse d'abord le texte en clair. Ensuite, il crée une clé de session, qui est une clé secrète à usage unique. Cette clé de session crypte les données. Lorsque les données sont chiffrées, la clé de session est ensuite chiffrée avec la clé publique du destinataire.

Cette clé de session chiffrée par clé publique est transmise avec le texte chiffré au destinataire.

Je couvre PGP plus en détail au chapitre 8, où vous créez vos clés privées et publiques, chiffrez un message et l'envoyez à un ami qui déchiffrera ensuite le message.

Cryptographie à courbe elliptique

La cryptographie à courbe elliptique, également connue sous le nom d'ECC, est une forme très différente de cryptographie asymétrique. Il n'est pas très utilisé, mais lorsqu'il l'est, il a tendance à être utilisé pour chiffrer de grandes quantités de données. En effet, ECC calcule très rapidement et ne prend pas beaucoup de temps de traitement. ECC est également plus récent et moins bien compris que certains des autres algorithmes de chiffrement. Pour cette raison, moins de chercheurs ont passé beaucoup de temps à essayer de les attaquer pour trouver leurs faiblesses. Je les mentionne ici parce que j'ai commencé à voir des programmes de stockage de données sécurisés utiliser ECC pour chiffrer les énormes quantités de données qui se trouvent dans de grandes fermes de serveurs.