Comment crypter des informations

Informations destinées à l'enseignant

Mandat 	Sur l'internet, des tiers peuvent avoir accès à nos données (courriels ou fichiers virtuels en pièces jointes). Les élèves apprennent ici à utiliser un logiciel de cryptage pour protéger documents et courriels.
Objectif 	Prendre conscience du fait que des tiers non autorisés peuvent accéder à notre correspondance et à nos documents sur l'internet. Apprendre à utiliser un logiciel de cryptage.
Matériel 	Logiciel de cryptage
Forme de travail 	Travail de groupe / travail individuel
Temps imparti 	20 minutes

Informations complémentaires

- Article sur l'histoire de la cryptologie: http://fr.wikipedia.org/wiki/Histoire_de_la_cryptologie

Comment crypter des informations

Lecture

Exercice	On a parfois besoin de communiquer des informations qui ne doivent pas tomber entre les mains de tiers. Plusieurs méthodes permettent d'atteindre ce but, mais le principe est que les données doivent être cryptées. Lis le texte suivant et constate par toi-même: le cryptage des données est une technique qui n'a absolument rien de moderne !

Le cryptage des données

L'idée de rendre un texte illisible et impossible à identifier pour des tiers est vieille comme le monde. Les scribes de l'Égypte ancienne, déjà, inscrivaient dans leurs textes des messages secrets en jouant sur l'ordre d'apparition des signes. Au Moyen-Âge, des écritures, voire des langues secrètes, étaient employées pour les échanges diplomatiques. Ces codes nécessitaient pour être compris une clé de chiffrement qui devait être remise au seul destinataire du message.

Alphabetum Kaldeorum est le nom de l'une des plus célèbres écritures secrètes du Moyen-Âge. Son nom renvoie aux Chaldéens, idéalisés au Moyen-Âge pour leurs connaissances en magie et en sciences occultes.

Ce code secret peut être consulté dans sa version intégrale à la bibliothèque universitaire de Munich. Il nous a été livré dans une écriture qui date de 1428, donc largement ultérieure à l'original, comme le prouvent quelques exemples qui témoignent de son application pratique.

L'Alphabetum Kaldeorum était destiné à l'origine à la correspondance diplomatique; le jeu de caractères montre que l'on chiffrait essentiellement des textes latins: il n'y avait pas de distinction entre les lettres u et v; il fallait utiliser deux v pour écrire w et il manquait la lettre j. L'alphabet prévoit plusieurs graphies différentes pour les lettres qui se répètent souvent dans le texte, de sorte que le texte codé ne puisse être déchiffré par le recours à l'analyse des fréquences. Des "lettres" dépourvues de signification étaient également intégrées au texte chiffré afin d'en rendre le déchiffrement un peu plus difficile.

On attribue cet alphabet au duc Rodolphe IV d'Autriche (1339–1365), lui-même ayant fait passer ces signes pour étant d'origine indienne. Cette écriture semble en tout cas avoir été inventée de toutes pièces, et l'on ne retrouve aucune similitude avec les écritures employées en Inde.

Même le cénotaphe de Rodolphe IV , exposé à la cathédrale Saint-Étienne de Vienne, porte une épitaphe en langage codé. Celle-ci indique simplement son nom et son titre, rédigé avec l'Alphabetum Kaldeorum. C'est dire l'intérêt de Rodolphe IV pour le chiffrement !

Comment crypter des informations

Lecture

Exercice À quoi ressemble le cryptage des données aujourd'hui ?

De nos jours, beaucoup de données sont chiffrées afin que seul le destinataire approprié puisse en décoder les informations. Les programmes informatiques qui servent à chiffrer des messages utilisent des algorithmes complexes. Le chiffre le plus simple remonte à l'empereur romain Jules César, qui s'en servait pour sa correspondance, et porte donc le nom de code de César. Dans sa forme la plus simple, il consiste à décaler l'alphabet de trois rangs, de sorte à faire correspondre le A avec le D, le B avec le E, etc.

Que veut dire la phrase suivante, déchiffrable avec un simple code de César ?

LO HVW LPSRUWDQ GH FKLIIUHU VHV FRXULHOV

Exercice

Rédige un texte codé en t'aidant d'un système de cryptage spécial. Demande à ton ou ta camarade de classe de déchiffrer ce texte. Si la tâche s'avère ardue, donne-lui un coup de pouce !

Bien entendu, cette forme de cryptage ne suffit plus de nos jours à protéger l'accès à notre compte bancaire ou à d'autres informations confidentielles.

Les programmes informatiques sont aujourd'hui suffisamment performants pour résoudre ces problèmes. Certains peuvent même être téléchargés gratuitement sur l'internet.

Comment crypter des informations

Lecture

En conclusion, si tu souhaites envoyer des textes ou autres informations en toute sécurité, tu peux les chiffrer avec de tels programmes. Mais attention: le destinataire du message doit disposer du même programme que toi.

Voici quelques liens où trouver des programmes de cryptage:

PowerCrypt

TrueCrypt est un utilitaire de cryptage gratuit et Open Source qui met en œuvre les algorithmes de cryptage les plus puissants du marché en toute simplicité. Vous pouvez créer un disque virtuel qui sera stocké dans un fichier ou crypter l'intégralité d'un disque ou d'une partition existant.
http://truecrypt.softonic.fr/

Challenger 2.3.1.0

Challenger est un outil de cryptage fonctionnant via deux mécanismes. Le premier est une simple phrase en guise de mot de passe, qui peut être aussi longue que vous le désirez. Le fait d'utiliser une phrase permet à la fois un mot de passe très long, et très facile à retenir. Le second est un cryptage par un nombre très long, totalement aléatoire, qui ne dépend pas de votre ordinateur. Le logiciel fonctionne soit par glisser-déposer du fichier à crypter dans son interface, soit par clic droit, soit par accès depuis la barre des tâches.

http://www.clubic.com/telecharger-fiche193334-challenger.html

ViPNet Safe Disk

Ce programme crypte en effet vos données dès leur mise en mémoire sous forme de containers virtuels vous mettant à l'abri des tentatives de captures de vos données.

http://www.clubic.com/telecharger-fiche182104-vipnet-safe-disk.html

Comment crypter des informations

Solution

Solution Décryptage de la phrase écrite en code de César

Phrase décryptée:

Il est important de chiffrer ses courriels