DAILY SCIENCE
DÉCOUVREZ LA SCIENCE, LA RECHERCHE ET L'INNOVATION "MADE IN BELGIUM"

A MONS, LA CRYPTOGRBQIJF T'FYQPTF...

Publié le 26 janvier 2018

par Christian Du Brulle

« À Mons, la cryptographie s'expose ». Notre titre, à moitié « crypté » de manière simple (nous avons décalé quelques lettres d'une place dans l'alphabet à partir du « a » dans le mot « cryptographie »), nous entraîne dans une visite qui ravira les curieux d'histoire autant que de technologies et bien entendu aussi de… secrets.

Médical, professionnel, commercial, militaire: le secret est partout. Et pour le préserver, rien de tel que de « coder » ses informations. La pratique ne date pas d'hier.

La cryptographie, l'art de rendre une information incompréhensible à ceux auxquels elle ne s'adresse pas (et qui ne disposent pas de la clé pour la déchiffrer), est une pratique aussi ancienne que l'écriture. De l'Antiquité à nos jours, on lui connait même quatre périodes:

- - La cryptographie manuelle.
- - La cryptographie mécanique et électromécanique. Ce fut le cas de la fameuse machine Enigma allemande utilisée lors de la Première Guerre mondiale et dont les secrets ont été percés au jour par le mathématicien britannique Alan Turing.
- - La cryptographie numérique dans laquelle nous baignons actuellement.
- - Et demain la cryptographie quantique, celle tirant parti des états des atomes pour conserver le secret d'une information et son intégrité.

DAILY SCIENCE
DÉCOUVREZ LA SCIENCE, LA RECHERCHE ET L'INNOVATION "MADE IN BELGIUM"

Machine Enigma exposée au Mundanéum.

« Sans secret aucun, les gens pourraient voler les idées des autres, ou s'en inspirer. Ce mode de fonctionnement tuerait la spontanéité, la créativité et la démocratie, sans doute… » estime le cryptologue Jean-Jacques Quisquater.

La Belgique, pays de la cryptographie

Cet ingénieur civil en mathématiques appliquées (1970) et docteur en science informatique a été professeur à l'Université catholique de Louvain (UCL). Une de ses inventions se trouve dans nos portefeuilles. Il est l'inventeur des algorithmes de chiffrement qui cryptent les données de nos cartes d'identité, de nos passeports ou encore de nos cartes de paiement. Une nécessité dans le monde connecté que nous connaissons.

À ce propos, il n'est pas sans intérêt de rappeler, et l'exposition le fait à volonté, que la Belgique est un haut lieu de la cryptographie mondiale.

Un exemple parmi d'autres? Au 18e siècle, le diplomate José de Bronckhorst, Comte de Gronsfeld, mit au point son propre système de chiffrage: une amélioration du chiffre de César utilisant un décalage variable donné sous forme d'une clef numérique. Un peu comme le décalage des lettres dans le titre de cet article. Si ce n'est que José de Bronckhorst ne se contentait pas de décaler chaque lettre d'un même écart dans l'alphabet. Si sa clé de cryptage était par exemple 247, cela signifie qu'il décalait chaque première lettre de deux places, la seconde de quatre et la troisième de

DAILY SCIENCE
DÉCOUVREZ LA SCIENCE, LA RECHERCHE ET L'INNOVATION "MADE IN BELGIUM"

sept. Bien entendu, au plus longue est la clé, au plus confidentiel sera le message.

Vie privée, dark net…

Le Pr Quisquater est aussi le commissaire scientifique de l'exposition « Top Secret » proposée à Mons, au Mundanéum. L'expo décrypte l'histoire de ces techniques assurant la confidentialité de nos échanges.

Elle ne se limite cependant pas à une incursion profonde dans l'histoire de la cryptographie. Elle pose aussi la question de la protection de la vie privée sur Internet. Elle emmène également le visiteur dans les tréfonds du dark net.

Olivier Bogaert, Commissaire à la Police judiciaire fédérale, spécialisé en nouvelles technologies, est un des experts qui a prêté son concours à la mise sur pied de cette exposition. Lors d'une rencontre au Mundanéum, il en profite pour faire le point sur les principaux dangers du moment.

http://dailyscience.be/28/12/2015/surfez-tranquille-les-chercheurs-aussi-sont-concernes/

Dr Jekyll et Mr Hyde

« Sur le web, les attaques au logiciel rançonneurs occupent aujourd'hui le haut du podium », explique-t-il. « Ce logiciel malveillant qui infecte notre ordinateur, crypte les données qu'il contient et réclame une rançon pour obtenir une hypothétique clé de décryptage. Cette vague de problèmes aux logiciels rançonneurs est aussi liée à la diffusion de la multitude d'informations personnelles que nous diffusons sur le web, les réseaux sociaux, etc. ».

Comment s'en prémunir? Il faut être attentif à chaque message qu'on reçoit avant de cliquer sur un lien ou une pièce jointe. Et ce quel que soit l'appareil avec lequel nous communiquons. Le ransomware touche tous nos outils de communication: ordinateurs, tablettes, téléphones portables. Il se faufile jusqu'à nous de multiples manières. Par mail, bien sûr, mais aussi via des messageries, des applis théoriquement sécurisée ».

Le compte mail est devenu un coffre-fort numérique

Un autre conseil? « Penser à sauvegarder régulièrement vos données sur un disque dur externe, que vous débranchez de votre poste de travail une fois la sauvegarde terminée. Et puis, ne pas hésiter à changer et à bien sécuriser ses mots de passe. Je conseille d'utiliser une phrase de passe plutôt qu'un mot de passe. Cela ne met pas complètement à l'abri. Mais vu sa longueur, cela complique la vie des hackers. Ils mettront un temps plus long avant de le décrypter. Et si cela dure trop longtemps, il passera à autre chose… Le compte mail est devenu un coffre-fort numérique important. C'est à lui qu'il faut penser en priorité! »

Si la visite de l'expo vous motive à mieux sécuriser à l'avenir vos comptes en ligne, vos adresses mails, vos transactions sur le web, rien de plus facile. Rendez-vous sur Cybersimple, un site proposé par Test Achats et Google qui distille une série de conseils pertinents.

Et si vous pensez être déjà au top (secret) dans ce domaine, vérifiez facilement si c'est réellement le cas avec les petits tests proposés.

Lors de la visite de l'exposition, Olivier Bogaerts, le Commissaire de police spécialisé dans la cybersécurité, a répondu avec efficacité à toutes les questions posées dans ce test. Ce qui, manifestement, n'est pas le cas de tous les visiteurs.
Seuls 11% affichaient le même score que lui…

DAILY SCIENCE
DÉCOUVREZ LA SCIENCE, LA RECHERCHE ET L'INNOVATION "MADE IN BELGIUM"