Cryptographie

Aurèle Barrière & Nathan Thomasset

10 mars 2016

Mise en situation

Intérêt de la cryptographie

Cartes bleues Mail Transaction bancaires

Un codage ultime?

Seul quelqu'un qui connaitraît la clé pourrait décoder.

Exemple : chiffrement de César

Décalage.

Exemple.

Veni Vidi Decrypti

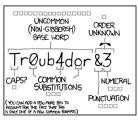
26 décalages possibles.

Énumération des clés

Énumérer les clés possibles (décalages). Regarder tous les résultats.

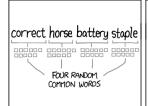
Complexité

Le calcul, c'est pas gratuit. Trop de clés -> trop de calcul, trop de résultats











EASY

DIFFICULTY TO GUESS: HARD



THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

D'autres exemples

Hill Vigenere

Analyse fréquentielle

Chiffres pour matrices de Hill Fréquences français

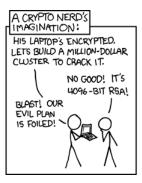
Cryptographie asymétrique

Clé publique, clé privée Mise en situation

RSA

Schéma

Limites





Ressources et idées

GPG mail sources des images