EPI

Bilan pour l'Oral DNB

I Définitions

La cryptologie, qui signifie la science du secret, regroupe la cryptographie et la cryptanalyse. C'est une science qui est apparue à la naissance de l'écriture et qui s'est développée avec l'apparition de grands empires toujours en lutte pour leurs frontières : la transmission sécurisée d'informations est devenue une priorité toujours plus importante pour les gouvernements et les individus. Cette science continue encore à progresser avec des codes toujours plus sécurisant. Il y a eu de grandes avancées notamment dans les années 1970.

La cryptographie consiste à crypter un message, c'est-à-dire le rendre illisible pour toutes les personnes excepté le destinataire du message.

La cryptanalyse cherche à décrypter un message sans en connaître la clé de chiffrement. On dit alors qu'on tente de « casser » le chiffrement.

II Utilités

La cryptologie a été très utile durant les différentes guerres. Par exemple, la machine Enigma cryptait des messages secrets pour l'Allemagne nazie et les Alliés, notamment Alan Turing, tentaient de les décrypter.

Cette science est aussi utilisée dans notre vie de tous les jours, afin d'assurer la confidentialité des communications et notamment la sécurité de toutes les transactions bancaires (utilisation des smartphone, paiement par carte bleue (RSA)...).

Il existe de nombreuses méthodes pour crypter un message soit en utilisant des clés privées, c'est à dire que si on connaît la clé on peut déchiffrer le message (comme les méthodes présentées ici César, Chiffrement affine, chiffre de Vigenère) ; soit en utilisant des clés publiques.

La cryptologie fait progresser et progresse avec les connaissances mathématiques (les nombres premiers par exemple) et informatiques (les capacités de calculs par exemple).

III Différents cryptages

Nous avons découvert, à travers des TP informatiques, trois méthodes de cryptage, la méthode de César, le chiffrement affine, qui sont deux méthodes de substitution monoalphabétique et le chiffre de Vigenère, qui est une méthode de substitution polyalphabétique.

En Devoir en Temps Libre, nous avons testé le codage de Polybe, ainsi que deux améliorations de ce code, dont une utilisée par les Allemands lors de la Première Guerre Mondiale.

IV Proposition de plan

Nous vous proposons un plan pour la présentation orale de cet EPI. Chacun est libre de l'utiliser, de s'en inspirer, ou d'en proposer un autre plus adapté à la présentation souhaitée et imaginée.

Plan

Introduction

I) Définitions (cryptologie, cryptographie, cryptanalyse)

II) Un événement historique dans lequel la cryptologie à jouer un rôle

III) Imitation Game (avec extrait si besoin, dilemme moral, Alan Turing)

IV) Proposer un code et un décodage (vu en cours ou personnel)
ou

IV) Mots de passe (en lien avec l'atelier lors de la venue d'Anthony Journault)

Conclusion : problèmes rencontrés, évolution de la cryptologie, ouverture vers un autre événement historique, ...

Vous retrouver l'ensemble des TP informatique sur le site Maths Alors !

Pour aller plus loin