MathsEnJeans

Sujet 5 : codes secrets

Le code de César.

Cette méthode a été utilisée par Jules César lors de ses correspondances secrètes.

Principe : il consiste à décaler dans l'alphabet toutes les lettres d'un texte, selon une longueur fixée appelée **clé** du code. Ainsi, en choisissant une clé égale à 2 par exemple, A est envoyée sur C, B sur D, etc. Notez que Z est envoyé sur B. Les mots du nouveau message codé y sont regroupés par blocs d'une longueur arbitraire.

Question 1 : combien de clés possibles existe-t-il ? Cette méthode de chiffrement est elle solide ?

Question 2 : déchiffrez le message suivant :

RWTGT RATDEPIGT HX IJ GTJHHXH P BT UPXGT RDCHIGJXGT JC EPAPXH TC IGDXH BDXH YT GTRDCCPXIGPX EJQAXFJTBRCI FJT IDC ETJEAT THI TCRDGT JC VGPCS ETJEAT BPXH Y TC SDJIT

Le code par substitution.

Principe : c'est une généralisation du code de César. Il consiste à attribuer à une lettre de l'alphabet une autre lettre, de sorte que chacune des 26 lettres de l'alphabet est codée par une lettre différente. Une clé correspond au choix d'une telle attribution, connue seulement de l'expéditeur et du destinataire.

Question 3 : combien y a-t-il de clés possibles ? Comparez avec le chiffrement de César.

Question 4 : le texte suivant a été codé par substitution. Saurez-vous retrouver son contenu ?

IWP PJTUIGAP IGTUP RWP KOGIGTP RW I JVAGCTW DIWPPWTA CGT NGWVQ R VTW IJTUVWVQ CGTGAGTW AGVA PVHHGNJTA WA DIWCW SVJTR I ZWVQW YW CW PGVKOWTP RWP YGVQP JTNOWTP WA YW FIWVQW WA YW C WT KJOP JV KWTA CJVKJOP SVO C WCFGQAW RWNJ RWIJ FJQWOI J IJ HWVOIIW CJQAW.

Question 5 : ce chiffrement est-il efficace pour de longs textes ?