

CRYPTOLOGIE

Cryptage symétrique

Aujourd'hui, de plus en plus de personnes étudient et travaillent à distance.

Mais lorsque nous utilisons Internet, il est important que nos données soient protégées.

Quelles catégories de données croyez-vous qu'il faille protéger en ligne ?

Comment pouvons-nous y arriver ?

Commençons par le message suivant :

KF TVJT VOF HJSM 4 UFDI

Pouvez-vous le lire ? Pourquoi ?

Si vous avez répondu parce qu'il est **codé** ou parce qu'il est **crypté**, vous avez raison !

Les codes de cryptage sont créés au moyen de fonctions mathématiques par des **cryptologues**.

Mastercard utilise des **clés** pour crypter les informations qui circulent sur son réseau.

Imaginez un cadenas.  Il vous faut une **clé** spécifique à ce cadenas pour le déverrouiller et le verrouiller.

Si la même **clé** permet de verrouiller et déverrouiller un message, il est protégé par un **cryptage symétrique**.

Cryptage
Conversion
d'informations
sous forme de
code, afin
d'éviter que des
personnes non
autorisées aient
accès à ces
informations

Symétrique
Deux éléments
identiques face
à face



CRYPTOLOGIE

Cryptage symétrique

Le **code ROT1** est un exemple de cryptage symétrique.

Vous faites une rotation d'une place pour chaque lettre.

A devient B.. B devient C.

Le code ROT1 est la **clé** qui a été utilisée pour coder le message.

KF TVJT VOF HJSM 4 UFDI

Pouvez-vous le lire maintenant ? Que dit-il ?

Essayez de coder un message personnel avec le code ROT1.

Demandez à des personnes si elles peuvent le décoder.

Il est possible que vous deviez communiquer votre clé !

Mais que se passe-t-il si quelqu'un devine, découvre ou vole votre clé?

Puisque la même clé est utilisée pour crypter et décrypter les informations, elles sont relativement faciles à décoder.

CODE ROT 1

LETTRE RÉELLE	LETTRE ÉCRITE
A	B
B	C
C	D
D	E
E	F
F	G
G	H
H	I
I	J
J	K
K	L
L	M
M	N
N	O
O	P
P	Q
Q	R
R	S
S	T
T	U
U	V
V	W
W	X
X	Y
Y	Z
Z	A

CRYPTOLOGIE

Tokenisation

Que se passerait-il si la relation entre les données et leur cryptage était totalement due au hasard ?

Si le code ne suivait aucun modèle prévisible ?

Regardons un autre message. Pouvez-vous lire ceci ?



Il dit T O K E N I S A T I O N

C'est une autre forme de cryptage qui peut protéger vos données.

Dans l'exemple ci-dessus, chaque lettre est remplacée par un jeton ou ici un émoji.

Quels autres types de **jetons** choisies au hasard pouvez-vous imaginer ?

Composez un message et cryptez-le avec vos propres jetons.

Utilisez votre imagination pour créer vos jetons dans le tableau ci-dessous. Vous pouvez choisir des symboles, des images et même des couleurs !

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Cryptez vos messages ici:

Demandez à des personnes si elles peuvent décoder votre message.

Maintenant, si vous comparez le **cryptage symétrique** avec la **tokenisation**, quelle méthode est la plus sûre ?

Imaginez une porte avec une serrure. Une seule clé pour entrer et sortir OU plusieurs clés et plusieurs serrures ?

Si vous croyez que la **tokenisation** est la méthode la plus sûre, vous avez vu juste.

Vous êtes une cryptologue Girls4Tech !

Tokenisation
La tokenisation est un processus qui remplace des données sensibles par des « jetons » ou « alias » non sensibles

ATTESTATION DE RÉUSSITE

Félicitations !

VOUS ÊTES MAINTENANT CERTIFIÉE



A handwritten signature in black ink, appearing to read "Michael Miebach".

Michael Miebach
CEO, Mastercard

A handwritten signature in black ink, appearing to read "Susan Warner".

Susan Warner
Founder, Kids4Tech