Fiche pédagogique

Activité : Introduction à la cryptographie.

Objectifs pédagogiques : Présenter la cryptographie, le principe du chiffrement et du déchiffrement.

Notions abordées : Scytale, chiffrement d'atbash, chiffrement par décalage (César), chiffrement par substitution.

Matériel nécessaire : 4 bâtons de diamètres différents, parchemins en scratch, 2 tables de chiffrement/dechiffrement, disques de chiffrement/déchiffrement par décalage

Niveau : A partir du cycle 3.

Déroulement : La cryptographie, un terme composé du préfixe "crypto-" issu de la racine grecque "kruptos" signifiant "caché" et du mot "graphie" dérivé du grec signifiant "écrire". La cryptographie est une technique d'écriture où un message chiffré est écrit à l'aide de codes secrets ou de clés de chiffrement. Cette activité se propose de découvrir des méthodes classiques de chiffrement et déchiffrement, tout en donnant quelques repères historiques. Elle se compose de plusieurs jeux successifs correspondant à des chiffrements de plus en plus complexes.

Scytale :

Cette méthode est une des premières techniques utilisées. Durant l'antiquité grecque, dès le sixième siècle avant notre ère, on utilisait des bâtons, appelés scytales, et des parchemins pour transmettre des messages.

Jeu :

- Diviser le groupe en 2 groupes
- Donner à chaque groupe 4 bâtons de diamètre différent.
- Donner un parchemin à chacun des groupes.
- Laisser les groupes enrouler le parchemin autour des bâtons et déchiffrer le message.
- Leur donner un parchemin vide pour qu'ils transmettent les messages entre eux.

Explication : On remarque que le message est compréhensible juste quand on l'enroule sur un seul bâton Ceci veut dire que pour pouvoir lire un message sur un parchemin il faut utiliser un bâton ayant le même diamètre que le bâton avec lequel on a chiffré le message. Cette méthode est plutôt simple à casser, faut juste changer le diamètre des bâtons jusqu'à avoir un message lisible

Atbash :

L'atbash est une méthode développée par les Hébreux au cinquième siècle avant J.-C. . C'est un chiffrement monoalphabétique, c'est-à-dire qu'une lettre est remplacée par une autre. Il consiste à inverser l'alphabet lors de l'écriture d'un message : les A deviennent des Z, les

B deviennent des Y, ..., les Y deviennent des B, et les Z deviennent des A. Ainsi le mot BONJOUR est chiffré en YLMIQFL. Le fait que ce chiffrement soit symétrique fait que la méthode de déchiffrement est ma même que celle de chiffrement : remplacer les A par des Z, les B par des Y, ..., les Y par des B, et les Z par des A. On a ainsi la table de chiffrement suivante.

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

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

Jeu : Sur un tableau on leur donne un mot codé en Atbash : exemple DECHIFFREMENT (qui se code WVXSRUUIVNVMG).

On explique aux participants le principe et on leur donne une table de chiffrement vierge pour qu'il puisse faire celle de l'atbash. On les laisse ensuite déchiffrer le mot.

FIGURE 1 – Une table de déchiffrement vide et une remplie pour Atbash.

On sépare ensuite les participants en différents groupes. Chaque groupe chiffre un message que les autres doivent déchiffrer.

Explication : Ce chiffrement est simple et le fait que chiffrer et déchiffrer se font de la même manière évite les erreurs du à une confusion entre ces deux méthodes. Il est cependant facile à casser comme tous les chiffrements monoalphabétique. (Voir analyse fréquentielle ci-dessous.)

Chiffrement par décalage :

Il s'agit toujours d'une méthode de chiffrement mono-alphabétique, mais elle implique un décalage de X positions dans l'alphabet. César fut l'un des premiers à utiliser cette technique pour communiquer avec ses soldats et transmettre des ordres. Il optait pour un décalage de X=3, signifiant que la lettre A devenait un D, le B devenait un E, et ainsi de suite. On obtient ainsi la table de chiffrement suivante pour le chiffrement de César.

A	B	C	D	E	F	G	H	I	J	K	L	M
D	E	F	G	H	I	J	K	L	M	N	O	P

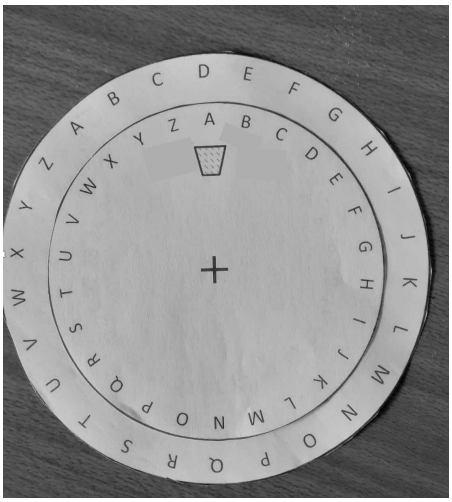
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Jeu :

- On commence par leur donner une table de chiffrement vierge et de la remplir pour un décalage de 3.
- On fournit tout d'abord un message à chiffrer. Par exemple, JE CHIFFRE PAR DECALAGE qui se chiffre en MH FKLIIUH SDU GHFDODJH.
- On fournit ensuite un message à déchiffer. Par exemple, IDFLOH D OLUH OH FRGH GH FHVDU qui se déchiffre en FACILE A LIRE LE CODE DE CESAR.
- On donne ensuite un message codé avec un autre décalage. Par exemple, HMFSLJRJSY, qui le chiffrement de CHANGEMENT, mais avec un décalage à 5, sans les prévenir. On laisse les participants trouver en les aidant si nécessaire.
- Enfin on leur demande de coder et décoder des messages avec des décalages divers.

Pour utiliser le chiffrement par décalage, on utilise un système avec deux disques concentriques superposés, un grand et un petit, à la circonférence desquels l'alphabet est écrit de manière régulière (une lettre tous les 26ème de tour).

En tournant, le petit disque de 3 crans jusqu'à ce que sa lettre A coïncide avec la lettre D du grand disque, on obtient la table de chiffrement. Pour chiffrer un message, on observe la lettre sur le petit disque et la remplace par la lettre correspondante sur le grand disque. Pour déchiffrer, on effectue l'inverse : on examine la lettre sur le grand disque et on la remplace par la lettre sur le petit disque.



Il est à noter que, comme l'alphabet à 26 lettres, ROT13 (décalage de 13 lettres) est le seul chiffrement par décalage pour lequel le chiffrement et le déchiffrement sont identiques.

Explication :

Les chiffrements par décalage sont faciles à casser. Si on sait que le chiffrement est par décalage alors on peut retrouver le message : il n'y a que 26 possibilités de décalage à tester (dont un, le décalage de 0 n'est pas vraiment un chiffrement) et de voir si l'une d'entre elles donne un texte qui a un sens.

Ils ont cependant largement été utilisés et jusque tard, par exemple par officiers sudistes pendant la Guerre de Sécession ou par l'armée russe en 1915. L'un d'entre eux ROT13 est encore utilisé de nos jours sur les forums internet. Le but est d'empêcher la lecture involontaire : (d'une réponse à une devinette, de la fin d'un film, ...).

Chiffrement par substitution mono-alphabétique :

Comme les chiffrements par décalage sont faciles à casser, on demande s'il ne serait pas possible de faire des chiffrements plus compliqués à casser. On fait réfléchir les participants en les guidant si besoin pour les amener aux chiffrements par substitution mono-alphabétique.

Dans un tel chiffrement, une lettre est remplacée par une autre (et une lettre n'en remplace qu'une) suivant une table de chiffrement sur la deuxième ligne de laquelle l'alphabet est écrit dans un ordre quelconque. On peut par exemple avoir la table suivante.

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

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

On peut leur faire chiffrer un message puis déchiffrer un autre, par exemple
KRT QRNWOC YC TC IRKKCOCI PXC GCOOC GRHOC qui se déchiffre en PAS FACILE DE SE RAPPELER UNE TELLE TABLE.

On demande ensuite combien il y a de tables possibles. On a 26 choix pour la lettre A, puis pour chacun de ces 26 choix 25 pour la lettre B (car une lettre est utilisée pour A), puis pour chacun de ces 26×25 choix 24 pour la lettre C (car deux lettres sont utilisées pour A et B), et ainsi de suite ... Il y a donc $26! = 26 \times 25 \times \cdots \times 2 \times 1$ soit environ $4 \cdot 10^{26}$ tables possibles (un nombre à 26 chiffres). Parmi elles, environ $1,5 \cdot 10^{26}$ (encore un nombre à 26 chiffres) sont telles que toute lettre est remplacé par une lettre différente d'elle même. Il est donc impossible d'essayer toutes les possibilités.

L'inconvénient est qu'il est difficile de se rappeler une telle table. Et si elle est conservée quelque part, l'ennemi peut éventuellement s'en emparer.