Masque jetable

Le masque jetable est le seul algorithme de cryptage connu comme étant indécryptable. C'est en fait un chiffre de Vigenère avec comme caractéristique que la clef de chiffrement a la même longueur que le message clair. Le système du masque jetable fut inventé par **Gilbert Vernam** en 1917, puis perfectionné par le major **Joseph O. Mauborgne** en 1918, qui inventa le concept de clef aléatoire.

Clair	M	A	S	Q	U	E	J	E	T	A	B	L	E
Clef	X	C	A	A	T	E	L	P	R	V	G	Z	C
Décalage	23	2	0	0	19	4	11	15	17	21	6	25	2
Chiffré	J	C	S	Q	N	I	U	T	K	V	H	K	G

Vernam Mauborgne

Méthode du masque jetable

Pour chiffrer un texte de manière sûre avec le chiffre de Vigenère, vous devez:

1. choisir une clef aussi longue que le texte à chiffrer,
2. utiliser une clef formée d'une suite de caractères aléatoires,
3. protéger votre clef,
4. ne jamais réutiliser une clef,
5. écrire des textes clairs ne contenant que les lettres (sans ponctuation et sans espaces).

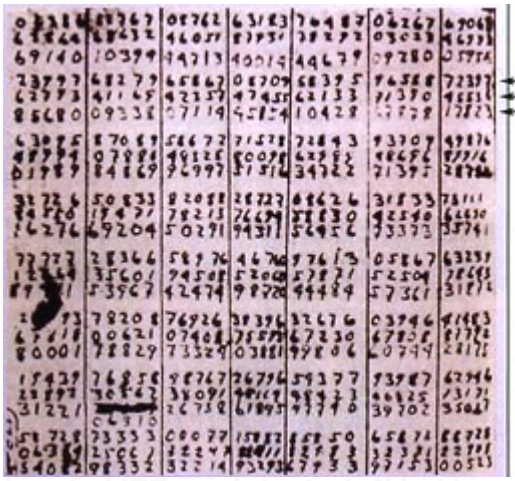
Le problème de ce système est de communiquer les clefs de chiffrage ou de trouver un algorithme de génération de clef commun aux deux partenaires. Un algorithme à base de cartes à jouer a été proposé récemment par Bruce Schneier: le Solitaire.

Le système du masque jetable, avec les précautions indiquées ci-dessus, est absolument inviolable si l'on ne connaît pas la clef. Il est couramment utilisé de nos jours par les États. En effet, ceux-ci peuvent communiquer les clefs à leurs ambassades de manière sûre via la valise diplomatique.

Lorsqu'en 1967 l'armée bolivienne captura et exécuta le révolutionnaire Che Guevara, les militaires trouvèrent sur son corps un papier montrant comment il préparait les messages qu'il voulait transmettre au président cubain Fidel Castro. Le Che utilisait le chiffre incassable inventé par Vernam. Les lettres du message du Che (rédigé en espagnol) étaient d'abord transformées en nombres décimaux selon la règle de substitution fixe suivante:

Clair	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
Chiffré	6	38	32	4	8	30	36	34	39	31	78	72	70	76	9	79	71	58	2	0	52	50	56	54	1	59

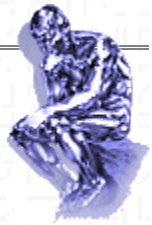
En elle-même, cette substitution ne procure aucune protection. Les chiffres du message mis à la suite sont ensuite découpés en blocs de cinq chiffres: c'est la ligne supérieure que l'on voit sur le document ci-dessous. La ligne du milieu est la clef, une séquence aléatoire de chiffres connue uniquement du Che et de Fidel Castro. Ensuite, le message et la clef sont additionnés (sans retenue, i.e. modulo 10), ce qui donne le message chiffré, la ligne inférieure de chaque groupe de trois lignes.
Pour déchiffrer, il fallait prendre le message chiffré, lui soustraire (modulo 10) la clef, puis faire la substitution inverse pour traduire les chiffres en lettres.



Cliquez pour agrandir


Fidel Castro et Che Guevara

Exercice:



Déchiffrement

Le message ci-dessous a été chiffré avec le chiffre du Che. La clef est le nombre π. Déchiffrez-le !

01237 55235 31127 12189 87479 1592

Décryptement

L'auteur des deux messages chiffrés ci-dessous n'a pas pris toutes les précautions qui s'imposent pour la sécurité totale du masque jetable: il a utilisé deux fois la même clef et de plus cette clef n'est pas aléatoire. Décryptez les messages ci-dessous, en essayant le mot probable "ennemi".

MYRWF AISPR AKOAL IOPHT LWUHP LZOWT WEWTR FOSFI FEJSC HJJD

ICXAE DMOPI YERWM CGAWN VREHP LZOWT WHHMN FOSFI UTKEB YWIPP UMAPH MHV