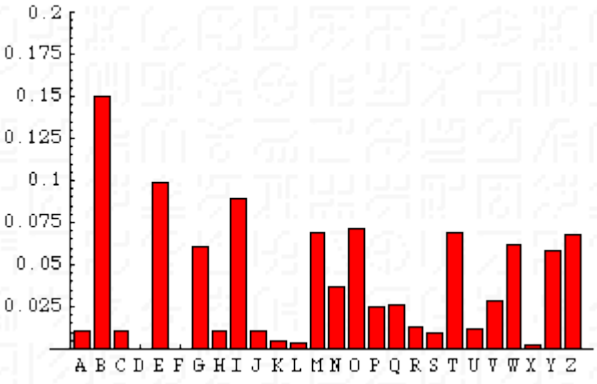
Le chiffre de Vigenère

Blaise de Vigenère (1523-1596), diplomate français, se familiarisa avec les écrits d'Alberti, Trithème et Porta à Rome, où, âgé de vingt-six ans, il passa deux années en mission diplomatique. Au début, son intérêt pour la cryptographie était purement pratique et lié à son activité diplomatique. Une dizaine d'années plus tard, vers 1560, Vigenère considéra qu'il avait mis de côté assez d'argent pour abandonner sa carrière et se consacrer à l'étude. C'est seulement à ce moment-là qu'il examina en détail les idées de ses prédécesseurs, tramant grâce à elles un nouveau chiffre, cohérent et puissant. Bien qu'Alberti, Trithème, Bellaso et Porta en aient fourni les bases, c'est du nom de Vigenère que ce nouveau chiffre fut baptisé, en l'honneur de l'homme qui lui donna sa forme finale.
Le **chiffre de Vigenère** est une amélioration décisive du chiffre de César. Sa force réside dans l'utilisation non pas d'un, mais de 26 alphabets décalés pour chiffrer un message. On peut résumer ces décalages avec un carré de Vigenère. Ce chiffre utilise une clef qui définit le décalage pour chaque lettre du message (A: décalage de 0 cran, B: 1 cran, C: 2 crans, ..., Z: 25 crans).

Exemple: chiffrons le texte "CHIFFRE DE VIGENERE" avec la clef "BACHELIER" (cette clef est éventuellement répétée plusieurs fois pour être aussi longue que le texte clair).

Clair	C	H	I	F	F	R	E	D	E	V	I	G	E	N	E	R	E
Clef	B	A	C	H	E	L	I	E	R	B	A	C	H	E	L	I	E
Décalage	1	0	2	7	4	11	8	4	17	1	0	2	7	4	11	8	4
Chiffré	D	H	K	M	J	C	M	H	V	W	I	I	L	R	P	Z	I

La grande force du chiffre de Vigenère est que la même lettre sera chiffrée de différentes manières. Par exemple le E du texte clair ci-dessus a été chiffré successivement M V L P I, ce qui rend inutilisable l'analyse des fréquences classique. Comparons les fréquences des lettres d'une fable de la Fontaine (Le chat, la belette et le petit lapin) chiffrée avec une substitution simple et celles de la même fable chiffrée avec le chiffre de Vigenère:



Substitution simple

Chiffre de Vigenère

On voit bien que l'histogramme n'a plus rien à voir avec celui d'une substitution simple: il est beaucoup plus "plat". Ce chiffre, qui a résisté trois siècles aux cryptanalystes, est pourtant relativement facile à casser, grâce à une méthode mise au point indépendamment par **Babagge** et **Kasiski**. Une autre méthode complètement différente a été encore mise au point plus tard par le commandant **Bazeries**.

Si la clef est aussi longue que le texte clair, et moyennant quelques précautions d'utilisation, le système est appelé masque jetable.

Exercices

Chiffrement

Chiffrez **à la main** le texte suivant avec le chiffre de Vigenère en utilisant le mot-clef "**Jeanne-Marie**":
Jeanne-Marie a des mains fortes, Mains sombres que l'été tanna

Déchiffrement

Déchiffrez **à la main** le texte suivant avec le chiffre de Vigenère en utilisant le mot-clef "**Jeanne-Marie**":

VEIAF TMLVA GXQMR QIEMR QRBQO EGIES FVXLI DRFQM IEAHN NUNAE

Vigenère sans clef secrète commune

Le chiffre de Vigenère tel que décrit ci-dessus exige, comme presque la totalité des systèmes de chiffrement, que les deux correspondants connaissent une clef secrète commune. Il est cependant possible, moyennant trois envois de message au lieu d'un, de se passer de clef commune.

Tentez de trouver la manière de faire...
