8. Le jeu de l'adversaire

Le jeu cryptologique comprend un adversaire avec qui il faut compter. Son but est le décryptement des messages, c'est-à-dire un déchiffrement sans la clé. Ce travail délicat est essentiel pour assurer la solidité d'un procédé. Comme l'avait déjà fait remarquer Charles Babbage, dans un échange du *Journal of the Society of Arts*, on ne peut proposer un chiffre sûr que si l'on a soi-même décrypté des chiffres très difficiles.

Il est admis aujourd'hui que les substitutions simples tombent rapidement sous les coups de l'analyse des fréquences. La technique utilisée a été exposée pour la première fois par le philosophe et mathématicien arabe Al Kindi dans son traité sur l'*extraction de l'obscur* dès le neuvième siècle.

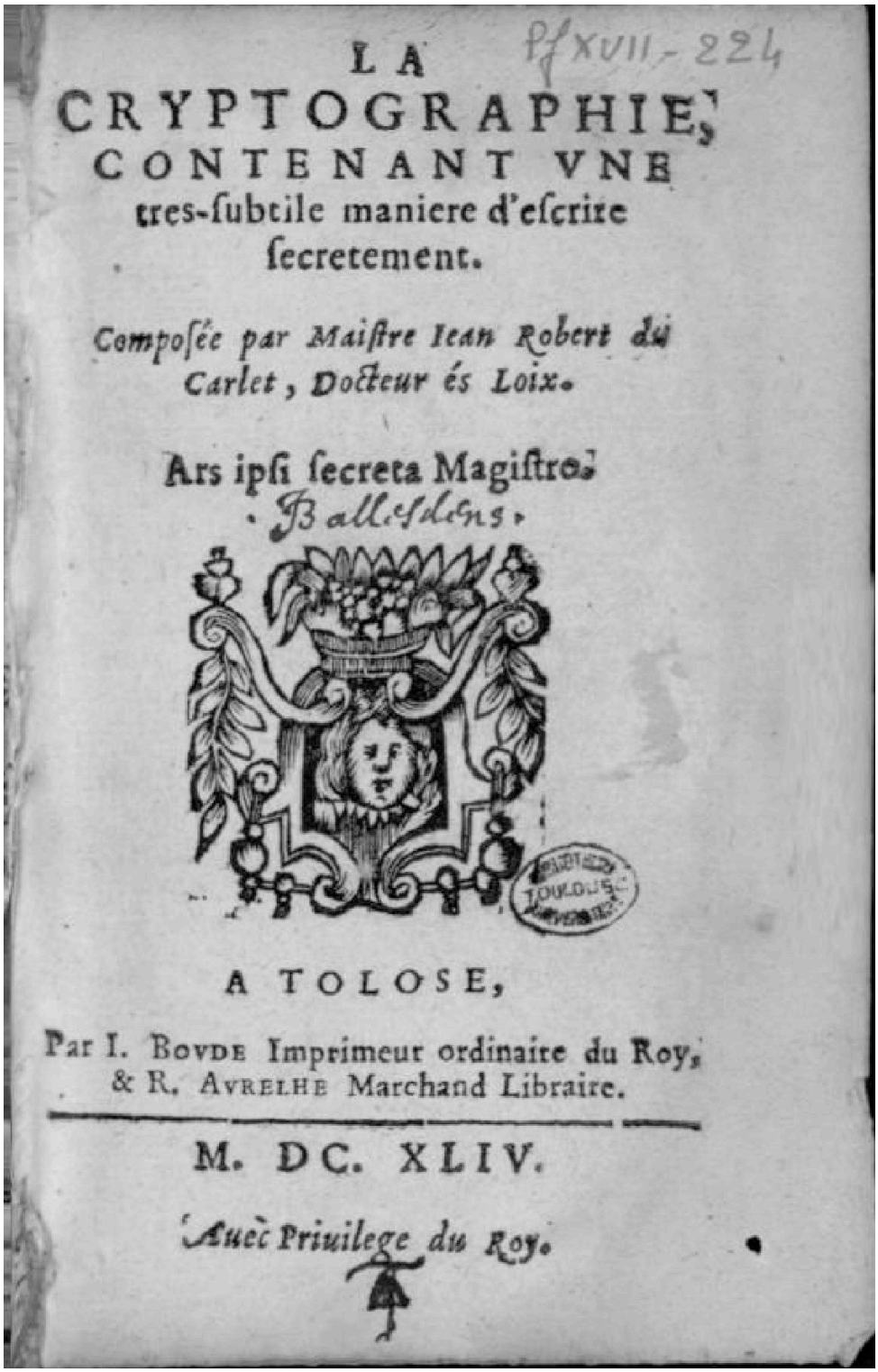
© http://dubsahara.com/oriental/musicians/historic/al-kindi

Le travail de décryptement comprend deux phases. L'une, quantitative, consiste à compter les occurrences de chaque caractère dans le texte dont on veut retrouver le sens, et la seconde, qualitative, consiste à utiliser la connaissance de la langue et l'intuition.

La nouvelle d'Edgar Poe, *Le scarabée d'or*, parue en 1843, décrit en détail de patient travail du décypteur. La méthode suit presque mot pour mot un article de David A. Conradus, *Cryptographie Denudata*, parue en 1842 dans le *Gentleman's Magazine*.

Les substitutions polyalphabétiques ont résisté plus longtemps à l'analyse. Il a fallu attendre le dix-neuvième siècle avec les travaux de Charles Babbage, puis de Friedrich Kasiski pour voir apparaître une méthode analytique de décryptement. L'étape cruciale est la détermination de la longueur de la clé. Elle est déterminée en repérant les répétitions dans le cryptogramme. Cette méthode a été affinée par William Friedman au début du vingtième siècle qui a utilisé l'index de coïncidence, défini comme la probabilité de collision d'un symbole dans le cryptogramme. Cette grandeur, significative de l'information portée par les lettres d'un texte, est connue aujourd'hui sous le nom d'*entropie de Rényi*. Elle permet de distinguer des caractères issus d'une langue naturelle d'une suite purement aléatoire.

L'adversaire est toujours supposé connaître le détail du procédé de chiffrement. Ce principe a été énoncé par le linguiste Auguste Kerckhoffs en 1882 qui prônait des méthodes qui ne devait pas reposer sur le secret du procédé, mais seulement sur celui d'une clé facilement modifiable. Sa thèse repose sur le principe que Jean-Robert Du Carlet, a apposé comme devise en tête de son ouvrage sur la cryptographie « *Ars ispsi secreta magistro* », un art caché au maître lui-même, signifiant qu'un chiffre n'est bon qu'autant qu'il reste indéchiffrable par son propre inventeur.



LA
CRYPTOGRAPHIE,
CONTENANT VNE
tres-ſubtile maniere d'eſcrire
ſecretement.

Compoſée par Maiſtre Iean Robert dit
Carlet, Docteur és Loix.

Ars ipſi ſecreta Magiſtro.

A TOLOSE,

Par I. Boude Imprimeur ordinaire du Roy,
& R. Avrelhe Marchand Libraire.

M. DC. XLIV.

Auec Priuilege du Roy.

http://tolosana.univ-toulouse.fr/notice/075574276

Outre la connaissance du procédé, le jeu cryptologique fournit aujourd'hui à l'adversaire un dispositif qui réalise l'opération de déchiffrement et qu'il peut observer, sur lequel il peut effectuer des mesures physiques, provoquer des erreurs de fonctionnement, afin qu'il puisse en extraire les secret. Il serait en effet indésirable qu'un lecteur de carte bancaire puisse en extraire les secrets, simplement par l'observation de sa consommation électrique, ou du temps passé aux calculs.

Par exemple, l'observation de la consommation d'une carte à puce peut révéler l'exposant privé utilisé pour un déchiffrement RSA. Fort heureusement, les fabricants de carte ont su trouver des

parades pour résister à ces attaques.

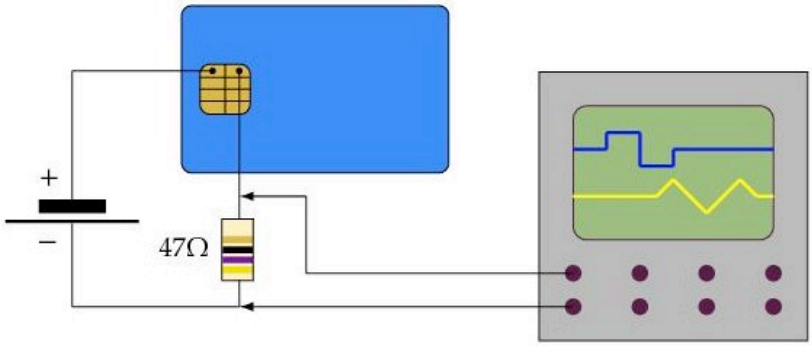


Fig. 4.4 Banc de mesure pour analyser la consommation d'une carte à puce pendant la réalisation d'un calcul cryptographique : la consommation du dispositif est mesurée et mémorisée en vue d'une analyse statistique. Un banc similaire permet de mesurer avec précision le temps d'exécution.

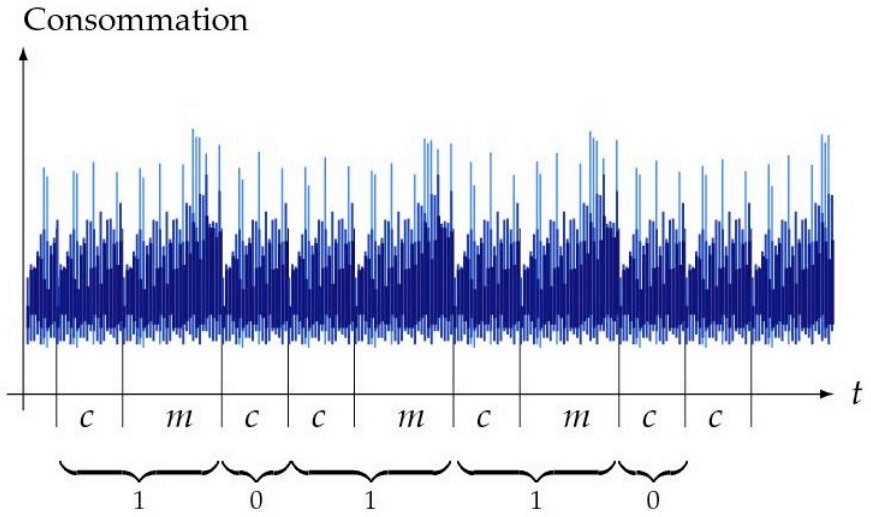


Fig. 4.5 Analyse de consommation sur un dispositif réalisant un calcul RSA. La courbe de consommation permet de discerner assez clairement les multiplications m des élévations au carré c. Cela dévoile directement les chiffres binaires de l'exposant privé.