Réalmont : une victoire obtenue par la seule arme du chiffre

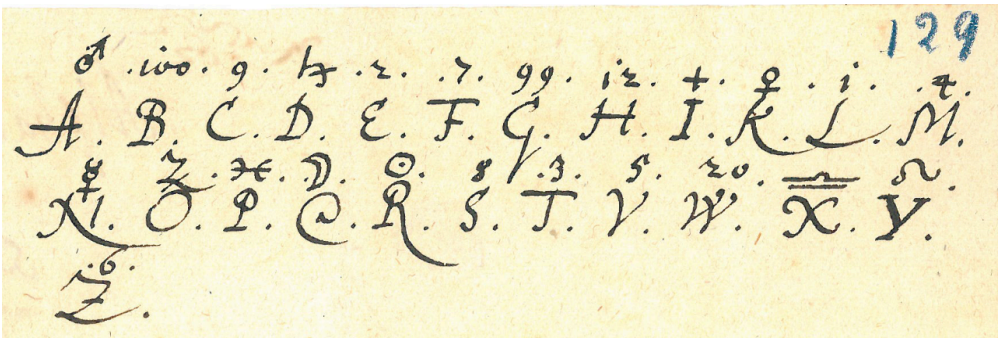
Le décryptement d'un seul message peut décider du sort d'une bataille ou d'une négociation. Ce fut le cas en 1626 quand les troupes du prince de Condé assiégeant Réalmont interceptèrent un messager sortant de la ville, porteur d'un message incompréhensible. **Condé fit venir un jeune professeur de mathématiques de la région, Antoine Rossignol des Roches, qui en trouva le sens**.

Le message annonçait que la ville était à cours de munition. Condé fit porter le message décrypté à la ville, qui se rendit. La bataille fut gagnée grâce à la seule arme du Chiffre !

Chiffrement par alphabet chiffré

Ce message avait vraisemblablement été chiffré au moyen d'un alphabet chiffré, où chaque lettre est remplacée par un symbole, très en vogue à l'époque. Le décryptement repose à la fois sur les mathématiques et sur la linguistique. Les mathématiques par la méthode des fréquences qui permet au moins de trouver le symbole représentant la lettre « e ». La linguistique par la méthode du mot probable qui permet de deviner des mots du message selon le contexte.

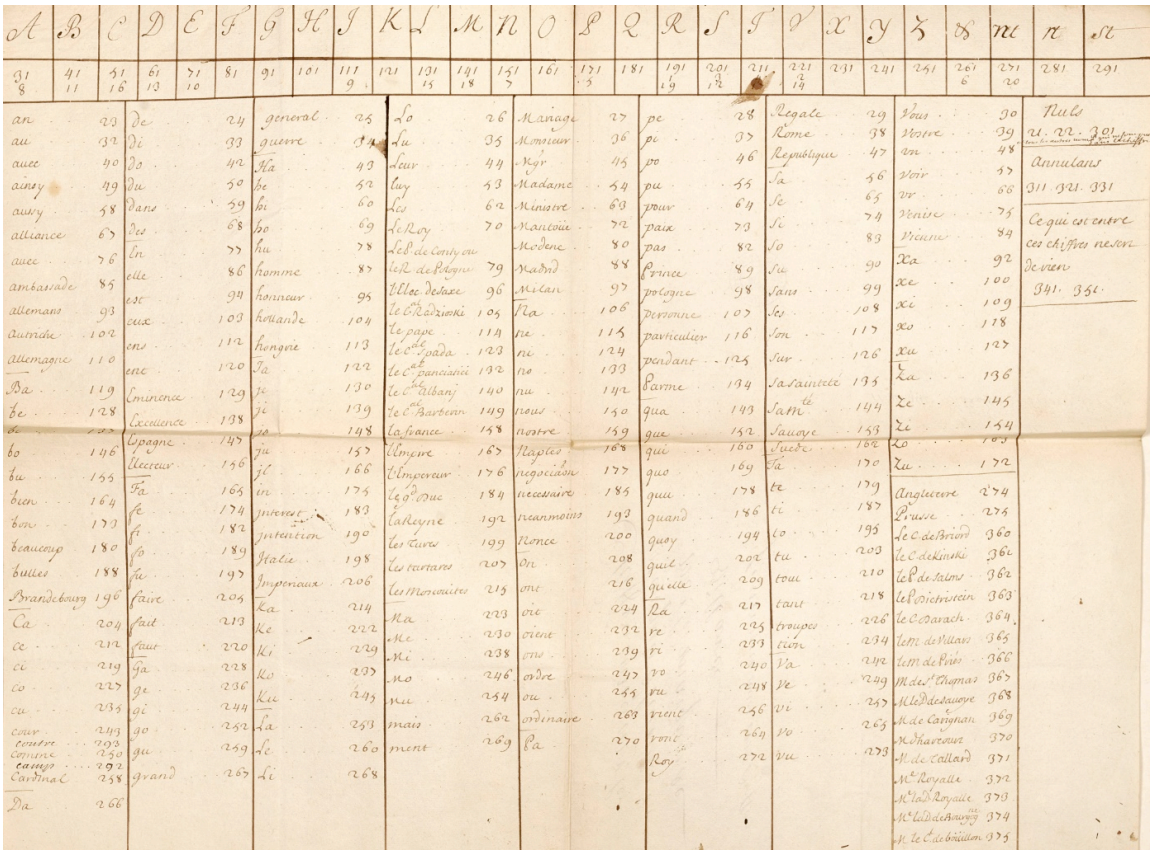
Par exemple, dans un message sortant d'une ville assiégée, on peut s'attendre à des mots comme « vivres » ou « munitions ».



Un alphabet chiffré de 1626. Chaque lettre doit être remplacée par le symbole inscrit au dessus.

Chiffrement par dictionnaire chiffré

La faiblesse des alphabets chiffrés, même améliorés en chiffrant de plusieurs façons différentes les lettres fréquentes et en ajoutant des nulles, c'est-à-dire des symboles ne signifiant rien, amena Rossignol à créer des dictionnaires chiffrés c'est-à-dire des dictionnaires bilingues dont l'une des langues est le français et la seconde, des nombres. Ainsi, on chiffre non seulement des lettres (et ce de plusieurs manières), comme auparavant, mais aussi des syllabes et des mots.



Un dictionnaire chiffré où les lettres, mots, syllabes sont chiffrés par des nombres.

La méthode des fréquences n'a alors plus aucun sens et celle du mot probable devient difficile à utiliser. Leur inconvénient principal est leur sensibilité à l'espionnage ou aux hasards de la guerre.