

Exemple : On veut coder « BONJOUR ».

On pose $p=53$ et $q=97$. On a donc $n = 53 \times 97 = 5141$. La clé publique $e=7$ (premier avec 52×96). [il faut trouver d qui vaut ici 4279]

Il faut maintenant chiffrer le mot. Le plus simple : B=2, O=15, N=14, J=10, U=21 et R=18. D'où BONJOUR= 2 15 14 10 15 21 18.

On pourrait appliquer le code sur chacun des sept nombres, mais cela ne servirait pas à grand chose car le codage serait assimilable à un code de substitution facilement décryptable avec une analyse de fréquences.

Aussi, on utilise une astuce classique : On écrit BONJOUR sous la forme :

002 151 410 152 118

On a $2^7 \equiv 128 \pmod{5141}$, $151^7 \equiv 800 \pmod{5141}$, $410^7 \equiv 3761 \pmod{5141}$, $152^7 \equiv 660 \pmod{5141}$ et $118^7 \equiv 204 \pmod{5141}$. Et on renvoie la séquence codée : 128,800,3761,660,204.

Essayez de décoder le message que je vous ai concocté avec le même codage:

A décoder :

2237, 2718, 4179, 204, 755, 1311, 2723, 3763, 4179, 3935, 2723, 2980, 4016, 1657, 1722, 2912.