La lettre de John Nash à la National Security Agency

- Extra-muros -

Date de mise en ligne : mardi 21 février 2012

**
UREM :
Unité de Recherche sur l'Enseignement des Mathématiques**

John Nash, né en 1928, est un mathématicien brillant, Prix Nobel d'économie 1994, connu pour l'équilibre de Nash ainsi que pour sa schizophrénie mise en scène dans le film Un homme d'exception.

La NSA (Agence nationale de sécurité) vient de déclassifier une lettre manuscrite envoyée par John Nash en 1955 à propos d'une machine de chiffrement. Dans cette lettre, il explique les fondements théoriques des méthodes de chiffrement et de sa machine en particulier.

In this letter I make some remarks on a general principle relevant to enciphering in general and to my machine in particular.

...

Plus loin, il attire l'attention sur la distinction entre le temps de calcul polynomial et exponentiel, distinction essentielle dans la théorie de la complexité, rendue publique seulement dix ans plus tard.

So a logical way to classify enciphering processes is by the way in which the computation length for the computation of the key increases with increasing length of the key. This is at best exponential and at worst probably at most a relatively small power of ,

or

, as in substitution ciphers.

Lire la suite sur Turing's Invisible Hand