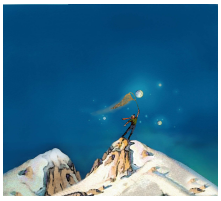


printemps des sciences

Avec le soutien de la Ministre de l'Enseignement supérieur et de la Recherche scientifique

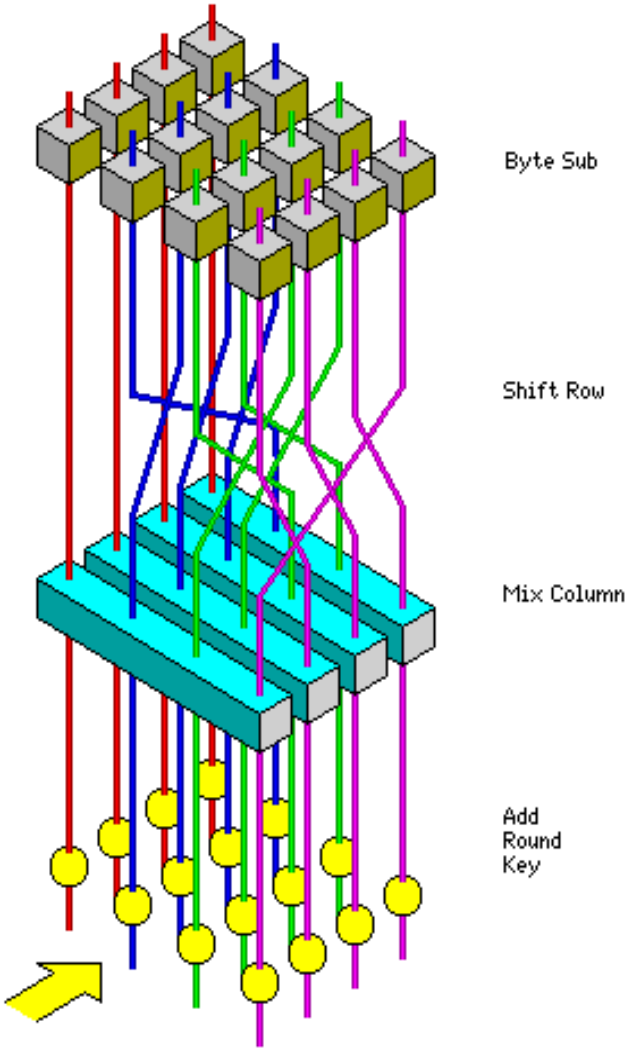
Sciences extrêmes 19 - 25 mars 2007

ULB

LA CRYPTOGRAPHIE

Fernandes Medeiros Stephane
Département d'Informatique

Schéma de l'AES :



L'AES, qu'est-ce que c'est ?

Il s'agit du nouveau standard de chiffrement, utilisé depuis l'année 2001. Il a été désigné par la NIST (Institut National des Standards et des Technologies, bureau américain) après un concours lancé en 1997. Il s'agit d'un chiffrement symétrique par bloc, d'origine belge.

L'AES, comment ça fonctionne ?

On distingue 2 grandes étapes :

- L'expansion de la clé
- Les tours de chiffrement qui comportent 4 transformations :
  - ByteSub
  - ShiftRows
  - MixColumns
  - AddRoundKey

Et la cryptographie ?

La cryptographie est la science visant à créer des cryptogrammes (= le message chiffré), c'est-à-dire à chiffrer. Le message peut prendre n'importe quelle forme : texte, image, son, vidéo, … On distingue deux types de chiffrement : symétrique et asymétrique. En informatique, on dispose de nombreux algorithmes pour chiffrer des données.

Est-on obligé de chiffrer de manière informatique ?

Non bien sûr, toute technique rendant une donnée inintelligible pour toute autre personne que son destinataire est également une technique cryptographique.