Explique moi... La science du secret

Sandrine Gauthier

Airbus Defence and Space

20 Mars 2019

AIRBUS

PARTIE 1

Mon parcours

- **Licence** mathématiques
  - **L1** & **L2** Mathématiques, Université Blaise Pascal (63)
  - **L3** Mathématiques Fondamentales et Appliquées, Université Paris-Sud (91) - **Magistère 1** de Mathématiques, Université Paris-Sud (91)

- **Master 1** Mathématiques Fondamentales, Université Paris-Sud (91) - **Magistère 2** de Mathématiques, Université Paris-Sud (91)

- **Master 2** Préparation à l'Agrégation, Université Paris-Sud (91)

- **Master 2** Algèbre Appliquée au Calcul Formel et à la Cryptographie, Université Versailles-Saint-Quentin-en-Yvelines (78) - **Magistère 3** de Mathématiques, Université Paris-Sud (91)

- Ingénieur sécurité et cryptographie, Airbus Defence and Space (78)

PARTIE 2

La science du secret

HISTORIQUE

- Techniques de dissimulation

- Exemples :
  - Tablettes de cire
    $\Rightarrow$ Cacher sur support contenant déjà de l'information
  - Tête d'un esclave
    $\Rightarrow$ Cacher physiquement

- Art du secret

- Exemples :
  - Transposition
  - Substitution
  - Cryptographie à clé privée / **symétrique**

- **Principe de Kerckhoffs** (1883)

- Cryptographie à clé publique / **asymétrique** (1976)
  - Diffie Hellman
  - Cryptosystème RSA

- Cryptographie quantique (1984)
  - Algorithme de Shor
  - Algorithme de Grover
  - Appel du NIST (2016 - 2022)

CRYPTOLOGIE

=

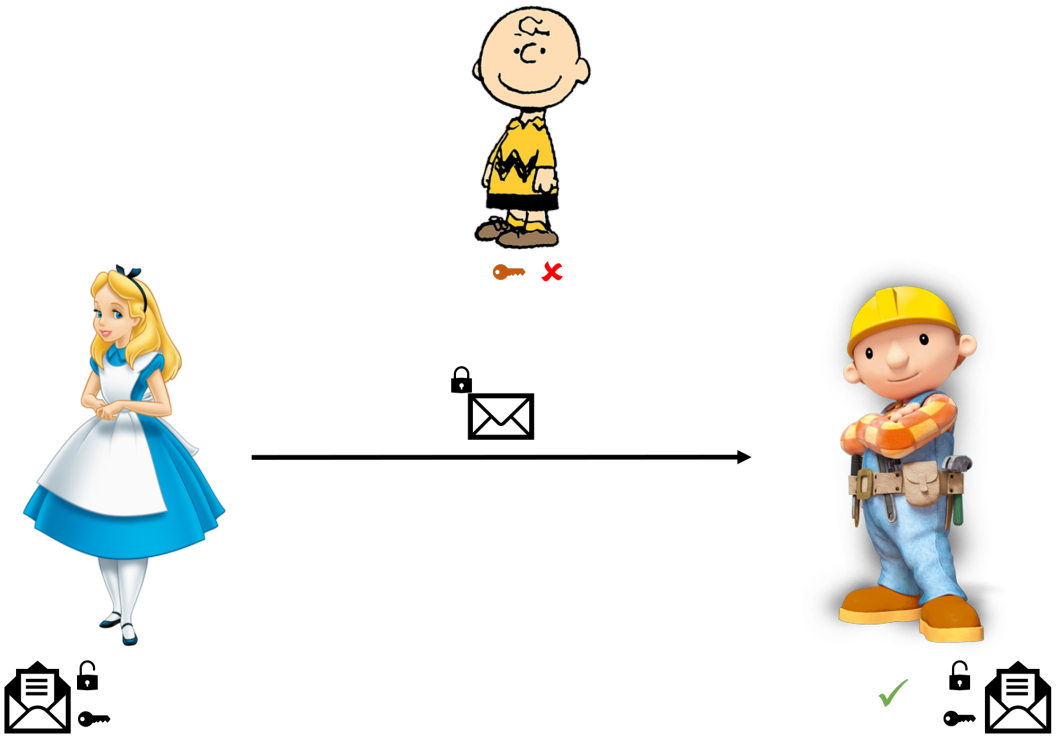
CRYPTOGRAPHIE + CRYPTANALYSE

Confidentialité : chiffrement
Intégrité : signature
Authenticité : signature, authentification

Analyse des protocoles cryptographiques

CRYPTOGRAPHIE SYMETRIQUE

- Clé **unique** pour *chiffrement* et *déchiffrement*



- Chiffrement par flot ou par blocs
- Calculs "rapides"

- Standard utilisé entre 1976 et 2001

- Alphabet $\mathbf{F}_2$
- Longueur de bloc 64 bits
- Clé 64 bits $\Rightarrow$ 56 bits

- Chiffrement :
  - Permutation initiale $\mathcal{P}$
  - Schéma de Feistel en 16 tours comprenant des boîtes de substitution (non linéaires)
  - Permutation inverse $\mathcal{P}^{-1}$

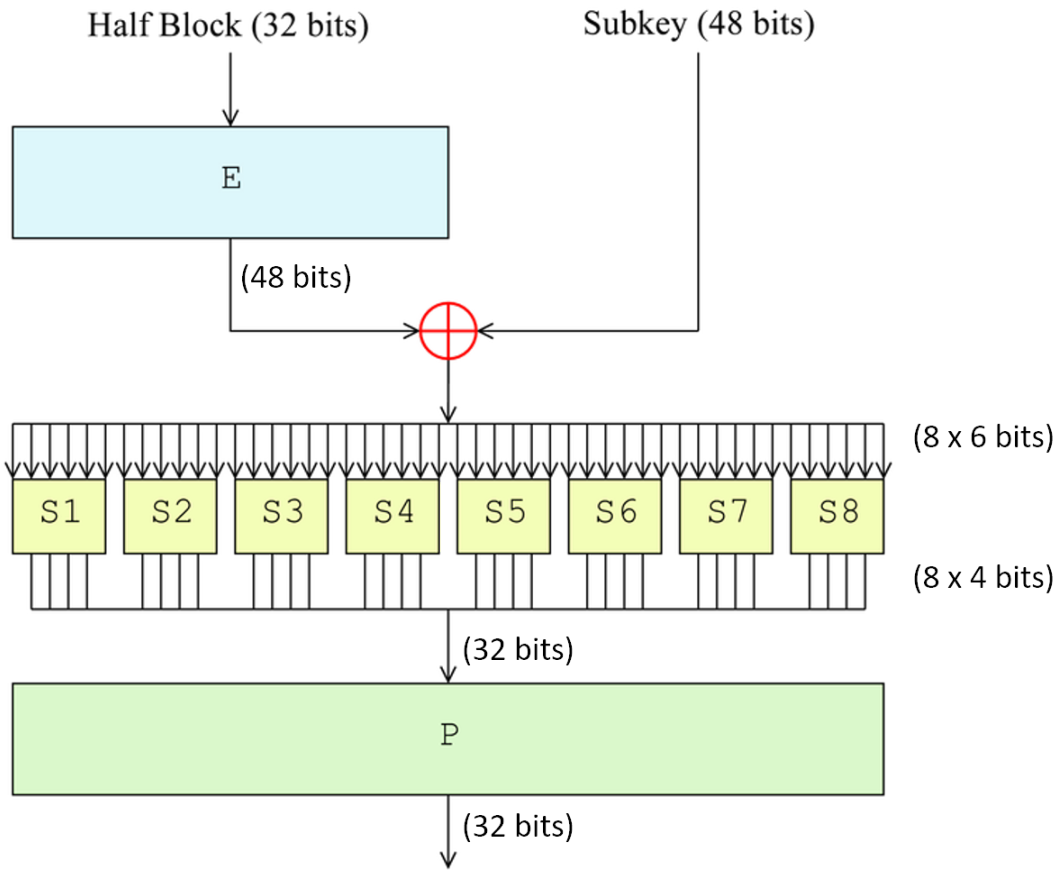


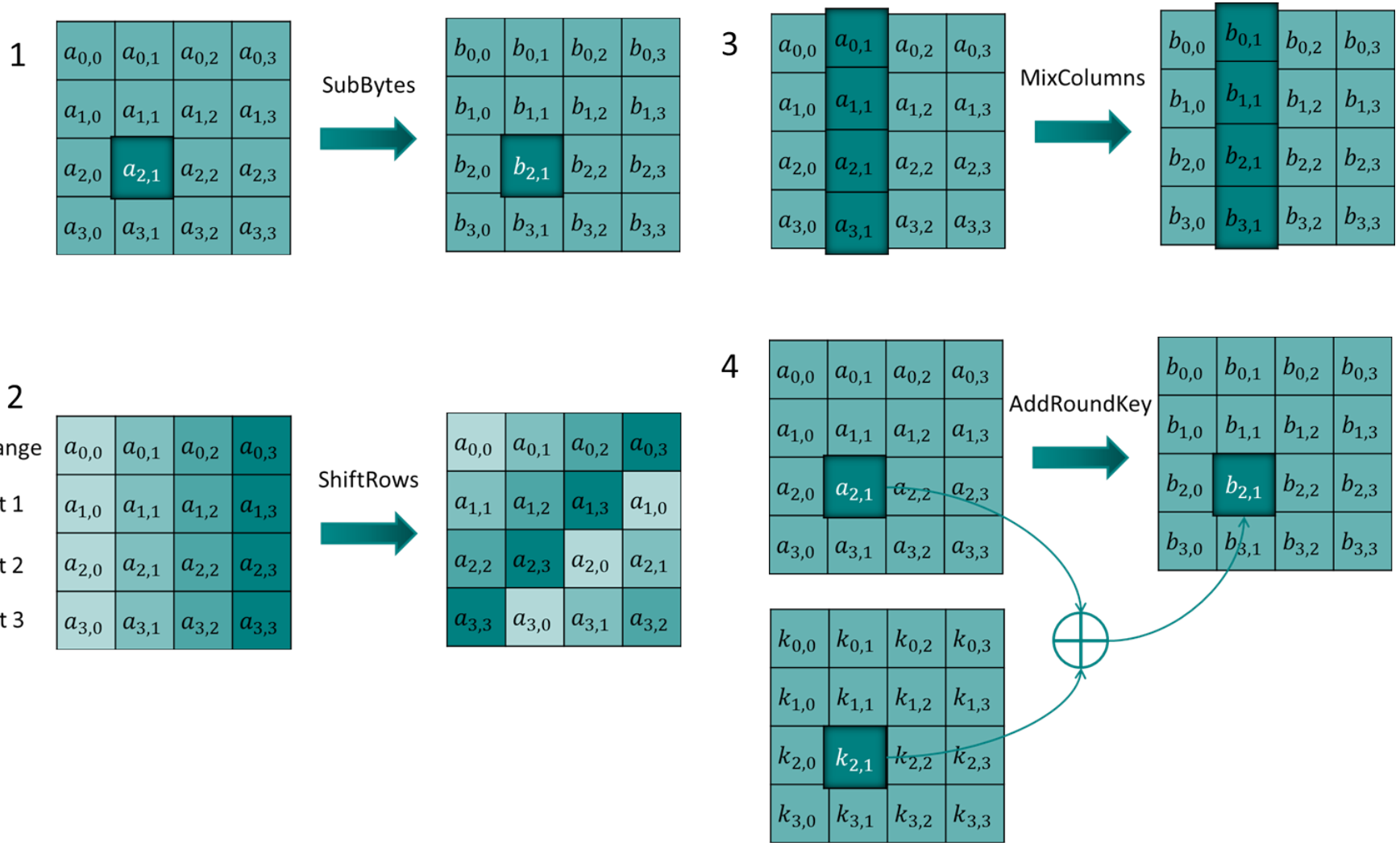
Figure – Transformation f_i du DES

- Standard utilisé depuis 2001

- Alphabet $\mathbf{F}_2$
- Longueur de bloc 128 bits
- Clé de 128, 192 ou 256 bits

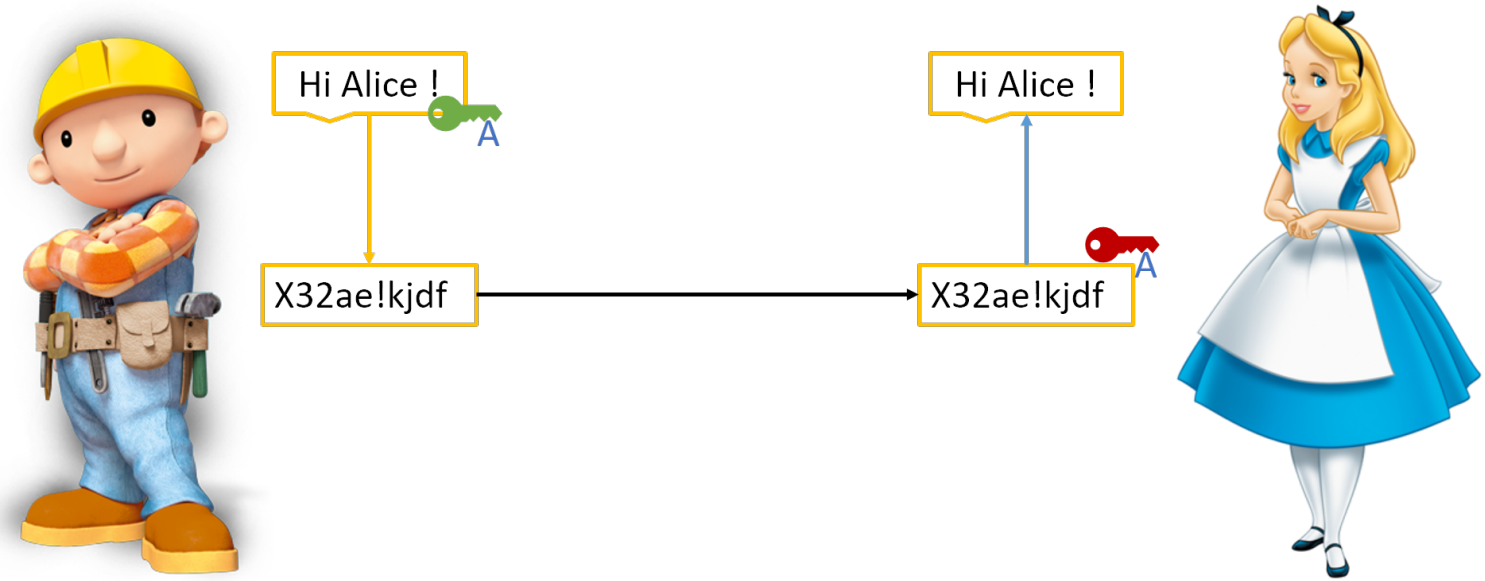
- Chiffrement
  - Addition initiale de la clé au message (linéaire)
  - Suivant la taille de clé, 10, 12 ou 14 tours de
    - Subbytes (non linéaire)
    - ShiftRow (linéaire)
    - MixColumn [sauf au dernier tour] (linéaire)
    - AddRoundKey (linéaire)

Advanced Encryption Standard



CRYPTOGRAPHIE ASYMETRIQUE

- Une clé **publique** pour le chiffrement **ET** une clé **privée** pour le déchiffrement



- Calculs "lents"

- Standard décrit en 1977 par Ronald **R**ivest, Adi **S**hamir et Leonard **A**dleman
- Chiffrement, signature et authentification
- Sécurité liée à la difficulté de factoriser un produit de deux grands nombres premiers

- Clé publique : $n = pq$, e
- Clé privée : p, q, $d = e^{-1} \mod \varphi(n)$
- Chiffrement : $c = m^e \mod n$
- Déchiffrement : $m = c^d \mod n$
- Signature : $s = m^d \mod n$

- Utilisé dans les cartes bancaires

CRYPTOGRAPHIE POST-QUANTIQUE

- Cryptographie symétrique :
  - Algorithme de Grover : recherche d'un élément en $O(n^{1/2})$ au lieu de $O(n)$
  - $\Rightarrow$ Doubler la taille des clés

- Cryptographie asymétrique :
  - Algorithme de Shor : factorisation d'un entier en **temps polynomial**
  - $\Rightarrow$ Casse les cryptosystèmes actuels

- Décembre 2016 : Appel à candidatures
- Novembre 2017 : Clôture des candidatures (69)
- 2017-2022 : Etude des candidats et sélection de nouveaux standards
  - Janvier 2019 : Candidats du 2nd tour annoncés

    17 (chiffrement) + 9 (signature)

PARTIE 3

Les débouchés possibles

- Métiers
  - Ingénieur cryptologue
  - Ingénieur sécurité
  - Ingénieur Recherche et Développement (sécurité et cryptologie)
  - Consultant sécurité
  - ...

- Secteurs d'activité
  - Cartes à puces
  - Télécommunications
  - Défense
  - Editeurs de solutions de confiance
  - Sociétés de conseil
  - ...

- Entreprises et organismes
  Airbus Defence and Space, IDEMIA, Thalès, Orange, Bull, Accenture, Ministère de la Défense,...

Exemples d'applications

- Paiement par carte bancaire sur un terminal
- Paiement en ligne
- Passeport biométrique
- Dossier médical partagé
- Vote électronique
- Cloud
- ...

Documentation

- Abonnement à la liste de diffusion crypto de l'ENS :
  - https://crypto.di.ens.fr/web2py/index/cryptolist
- Master Algèbre Appliquée au Calcul Formel et à la Cryptographie :
  - http://www.departement.math.uvsq.fr/master2AA
- NIST post-quantum cryptography :
  - https://csrc.nist.gov/Projects/Post-Quantum-Cryptography