Cryptologie

Introduction à la cryptographie — partie 2

Jean-Philippe Eisenbarth

H4ck 1n TN

November 4, 2015

Pourquoi utiliser la crypto aujourd'hui ?

Cryptographie symétrique

- Chiffrement par flot
- Chiffrement à bloc
  - AES
  - Mode Op : CBC

Cryptographie asymétrique

Souhait de toujours plus remplacer des services traditionnels par l'informatique.

- Communication
- Vote
- Notion de confiance

- Confidentialité

  Chiffrement

- Authenticité

  Signature

- Intégrité

  Hachage

- Cryptographie symétrique ou cryptographie à clé secrète.
- Plus ancienne ancienne forme de chiffrement.
- Chiffrement et déchiffrement avec la même clé.

2 types : chiffrement par flot, chiffrement à bloc

Chiffrement de Vernam, ou One Time Pad, ou Masque Jetable :

- le message est une suite de caractère (normal me direz vous ...)
- la clé doit également être une suite de caractère au moins aussi longue que le message
- on calcule un XOR bit à bit.

On obtient ainsi une suite de bit qui correspond au chiffré.

Pour déchiffrer on effectue un XOR entre les bits chiffrés et la clé (celle utilisée pour chiffrer)
On jette ensuite la clé (d'où le nom One Time Pad).

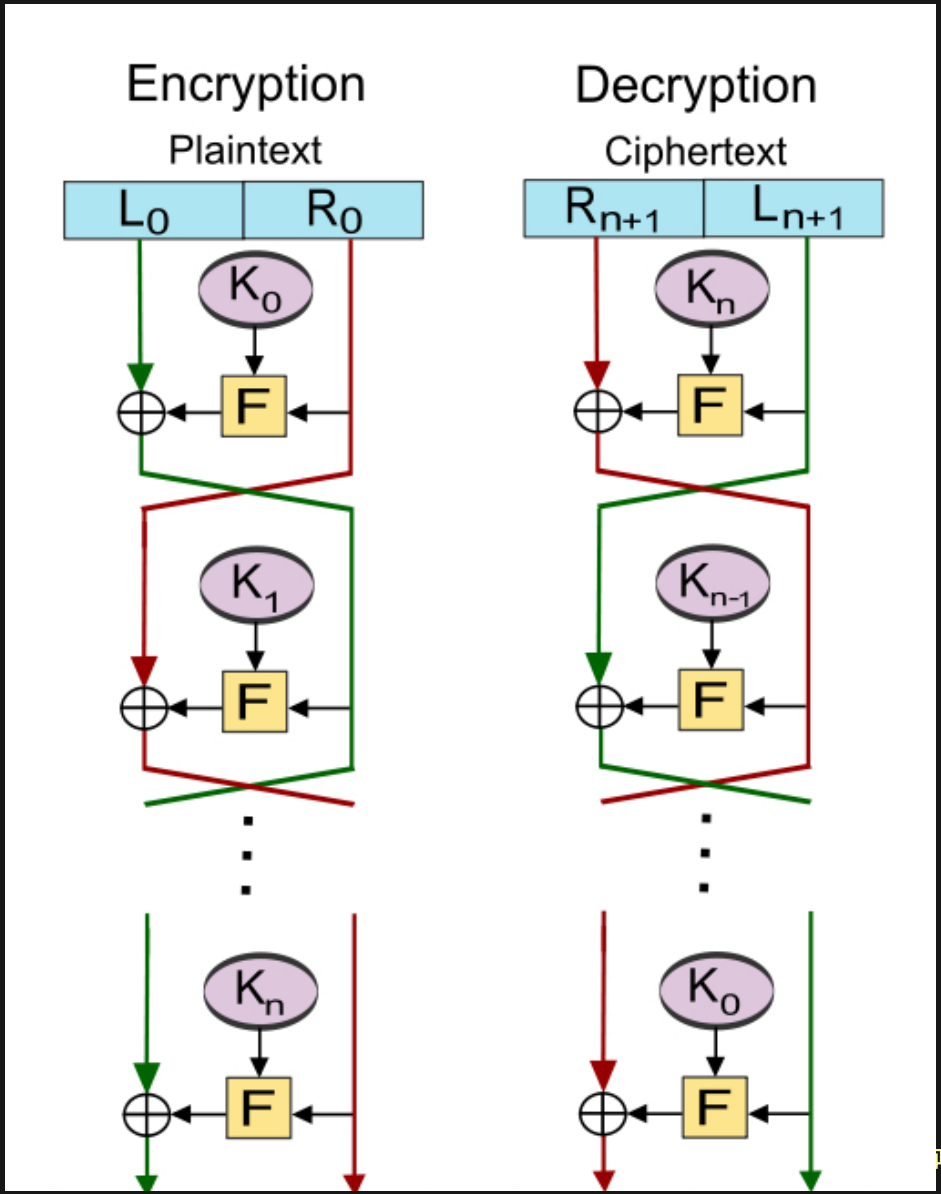
Toute l'astuce vient du caractère aléatoire de la clé.

La différence avec le chiffrement à flot (où l'on chiffre tout d'un coup) est que l'on chiffre par bloc.

Exemple : DES, AES, BlowFish

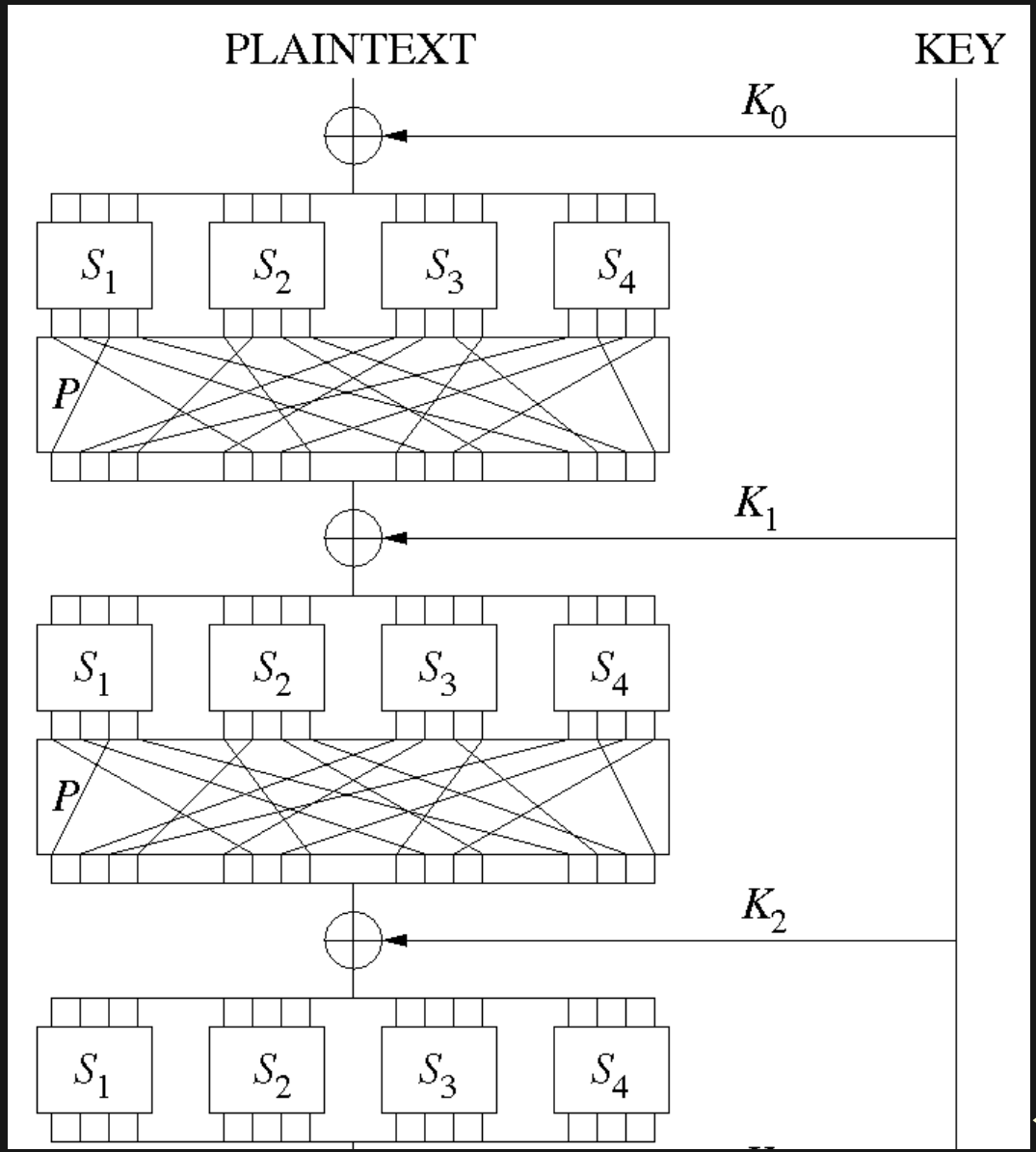
On peut transformer un chiffrement à bloc en chiffrement par flot en utilisant un mode d'opération spécifique.

Réseau de Feistel

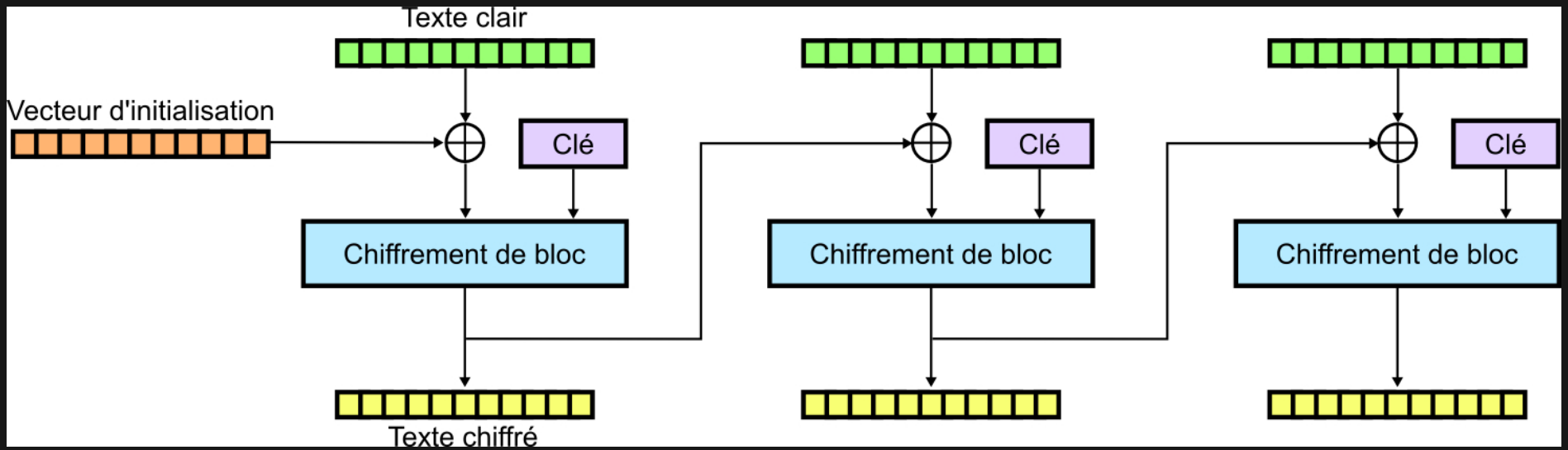


- Taille de bloc de 128 bits
- Taille de clé de 128, 192 ou 256 bits
- Seul le bruteforce peut en venir à bout (en des temps non raisonnables)

Réseau de substitution-permutation



Mode opératoire CBC (pour le challenge ;)



Cryptographie à clé publique

Chaque personne génère un couple <clé publique>, <clé privée>

Envoyer un message chiffré :

- Alice utilise la clé publique de Bob pour chiffrer un message pour lui
- Bob utlise sa clé privée pour déchiffrer le message

Signer un message :

- Alice utilise sa clé privée pour signer un message pour que Bob soit sûr que c'est bien Alice qui lui parle
- Bob utilise la clé publique d'Alice pour vérifier que c'est bien Alice qui a envoyé le message

Sources

Cours de M. Emmanuel Thomé (Cryptologie en 2A et Computer Security en 3A)