HE VD
IG

Y-CTF
STUDENT ETHICAL HACKING CLUB

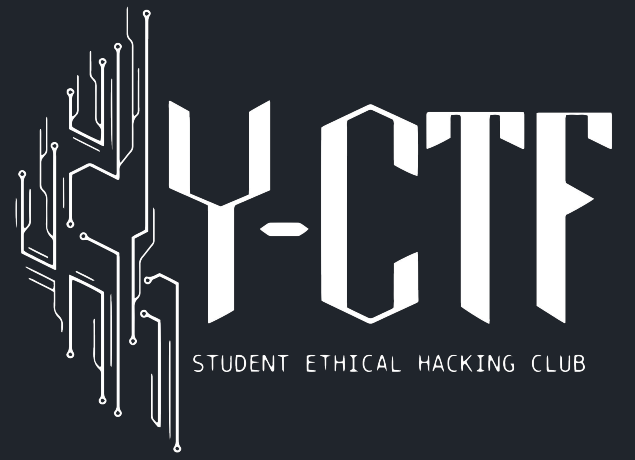
Cryptographie

Introduction

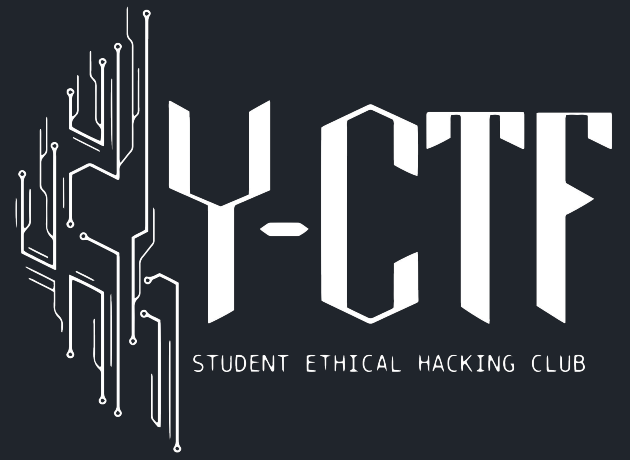
Workshop, présentation du 10.11.2021

Définition

- Techniques pour permettre des communications sécurisées
- Cherche à assurer (selon les cas)
  - Confidentialité
  - Intégrité
  - Authentification
  - Non répudiation



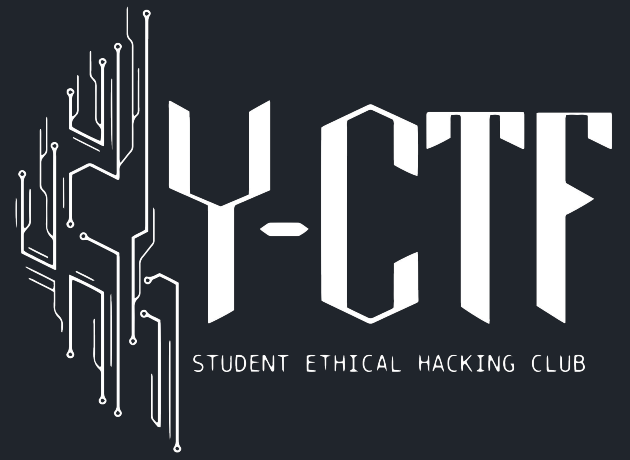
Aujourd'hui



Chiffrement symétrique

- Fonctionnement
- Mode d'opérations

Rappel



XOR

A	B	Y
0	0	0
0	1	1
1	0	1
1	1	0

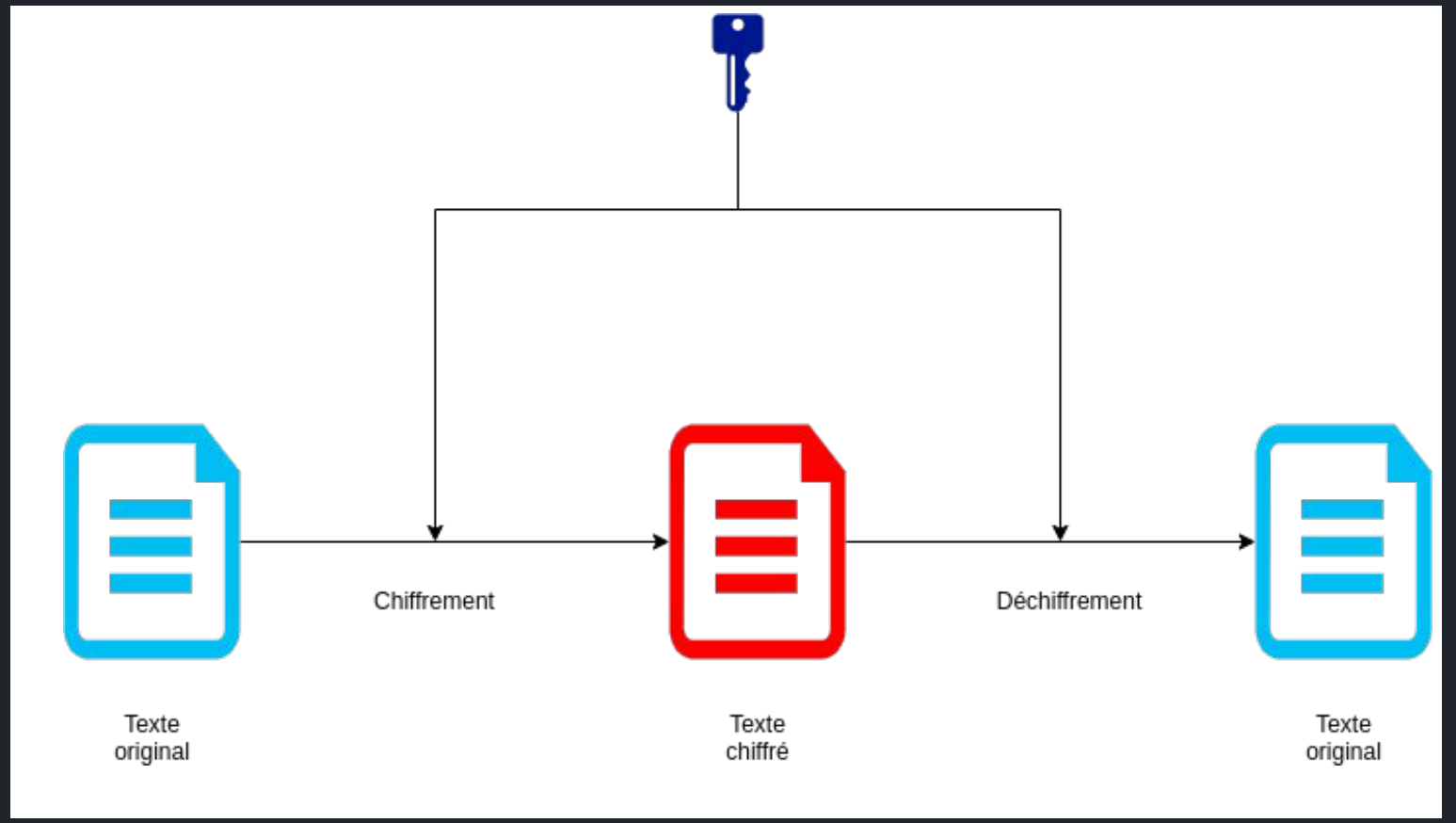
Fonctionnement

Fonction bijective

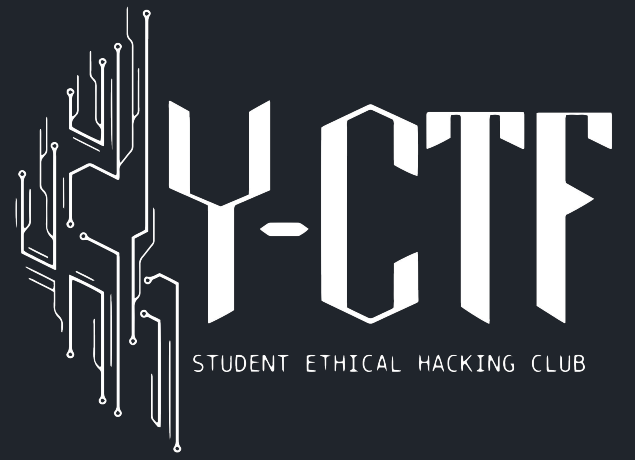
dépendante de la clé.

Difficile à casser sans la

clé.



Fonctionnement

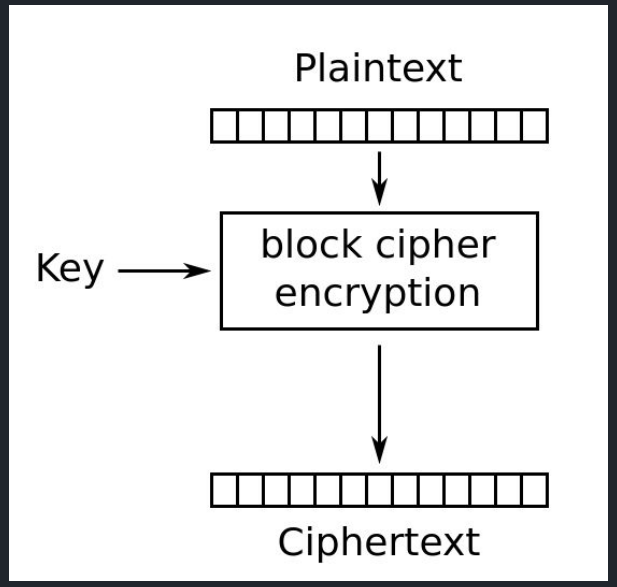


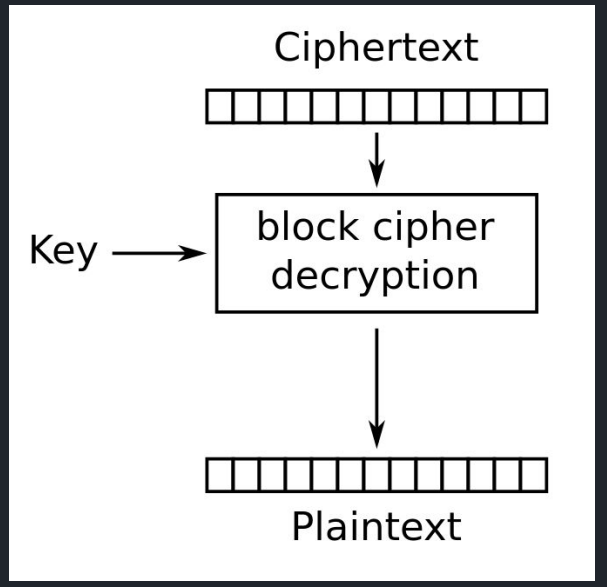
2 types de chiffrement

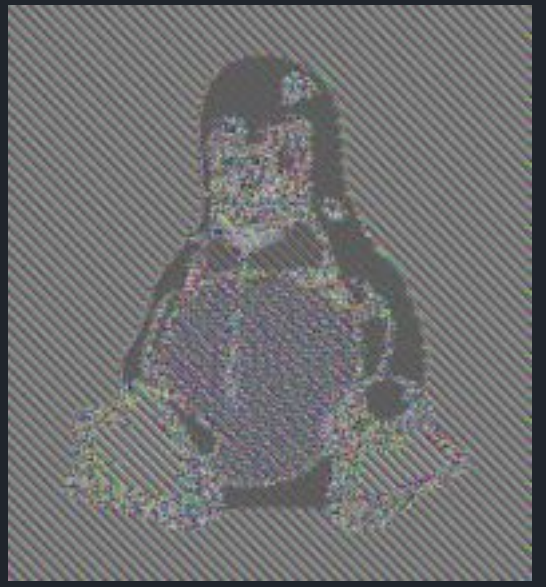
- Bloc
  - Texte est chiffré par l'algorithme
  - Chiffre uniquement des données de la taille de son bloc
- Flots
  - Le texte est XOR avec un flux généré par l'algorithme

Modes d'opérations (ECB)

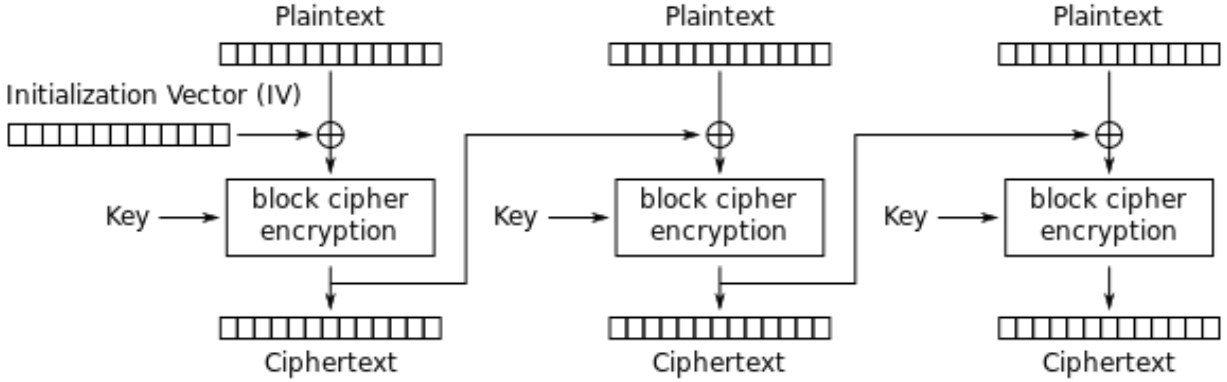
Pas de diffusion



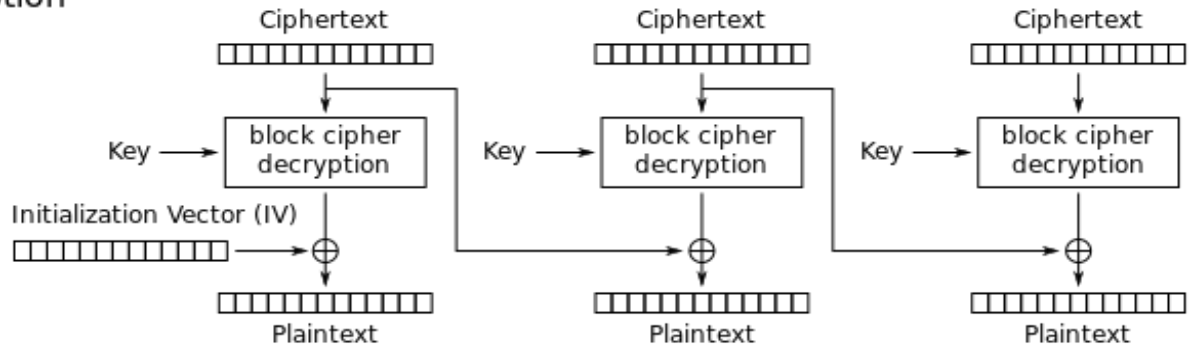




Modes d'opérations (CBC)



Cipher Block Chaining (CBC) mode encryption

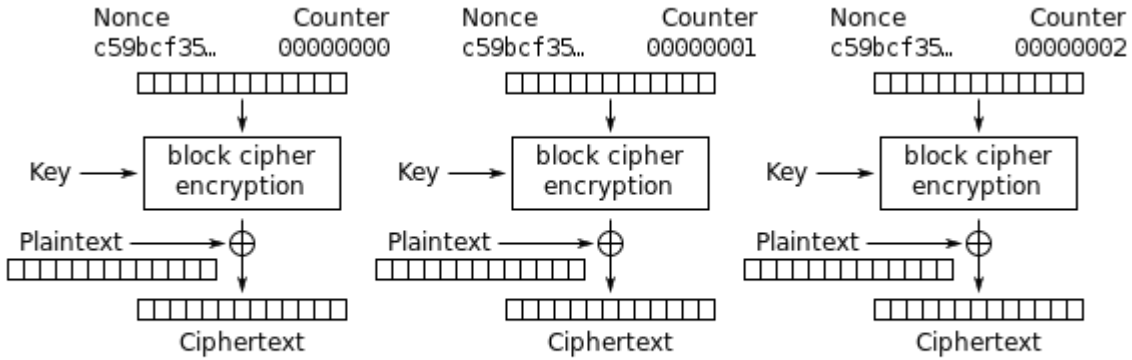


Cipher Block Chaining (CBC) mode decryption

Modes d'opérations (CTR)

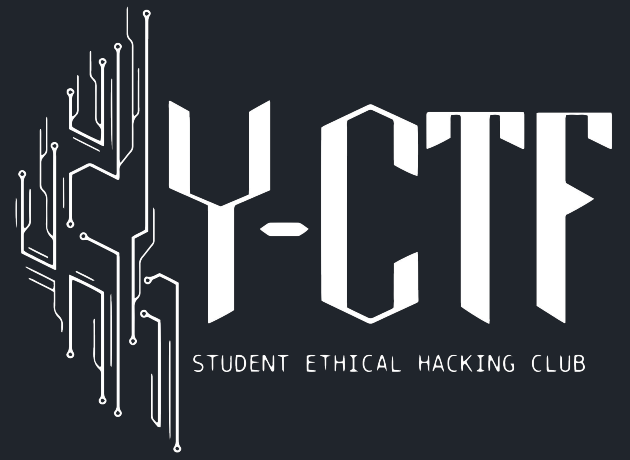
Bloc -> Flots

Comment déchiffrer ?



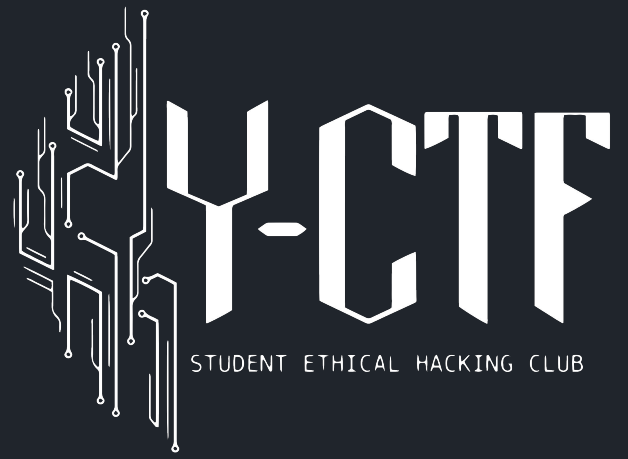
Counter (CTR) mode encryption

Clés et nonce



- Nonce/IV:
  - Pas un secret
  - Gestion très importante
- Génération des clés importante
- Régénérer la clé après un certain nombre de messages. (Birthday Attack)

Attaques



CBC: IV fixe

CTR: Réutilisation de l'IV

CBC: Bloc répétés

Mauvaise génération de clé