



DES PROGRÈS BIENVENUS EN CRYPTOLOGIE.

Groupe 2

...

Chiffrement des données



Nécessité

- Messages
- Mots de passes

Méthode actuelle



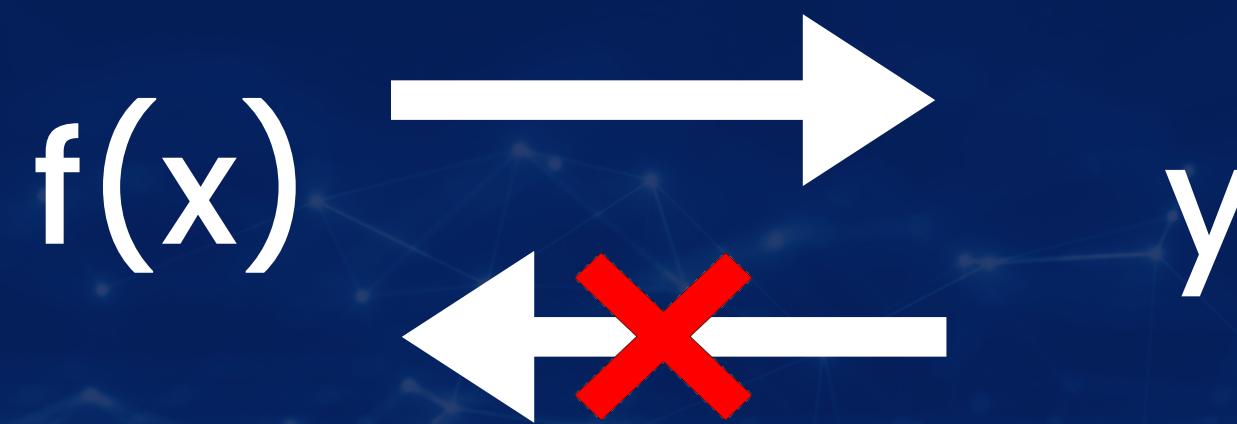
- Fonctions à sens unique
- Travaux de Levin
- Complexité de Kolmogorov
- Eventualités d 'Impagliazzo

...

Les fonctions à sens unique



Fonctionnement



Utilisations

- Transactions bancaires
- Communication en ligne

...

Complexité de Kolmogorov



- Permet de calculer la complexité d'un programme
- La complexité de Kolmogorov en temps limité en est une variante
- Utile pour démontrer l'existence de fonction à sens unique

...

Éventualités d'Impagliazzo



Algorithmica Heuristica



Permettent une
Cryptographie
sécurisée

Cryptomania Minicrypt



Ne permettent pas
une Cryptographie
sécurisée

...

En conclusion



- On ne peut toujours pas prouver l'existence des fonctions à sens unique
- Les avancées récentes ont permis de reformuler le problème
- Ces avancées nous mènent à une cybersécurité plus fiable