Chiffrement asymétrique Diffie-Hellman

Problematique

mathématiques

rincipe

Faiblesse d

Chiffrement asymétrique Diffie-Hellman

Christophe Viroulaud

Terminale NSI

Problématique

Le chiffrement symétrique est très efficace mais il souffre d'un défaut majeur : il faut que la source et le destinataire utilise la même clé de chiffrement.



Peut-on échanger une clé de manière sécurisée?

Chiffrement asymétrique Diffie-Hellman

Problématique

o'aider des mathématiques

Analogie des cou

Faiblesse d protocole

Les mathématiques à la rescousse

Chiffrement asymétrique Diffie-Hellman

Problématique

S'aider des mathématiques

Principe

Analogie des couleurs

Faiblesse di protocole

▶ 1974 : Le puzzle de Merkle s'appuie sur le coût long du décryptage.

Les mathématiques à la rescousse

Chiffrement asymétrique Diffie-Hellman

Problématique

'aider des nathématiques

Principe

Analogie des coule

protocole

- ▶ 1974 : Le puzzle de Merkle s'appuie sur le coût long du décryptage.
- ▶ 1976 : **Diffie et Hellman** utilise une fonction mathématique avec des propriétés particulières

Propriétés

Chiffrement asymétrique Diffie-Hellman

Problèmatique

S'aider des mathématiques

Principe

Analogie des couleurs

Faiblesse du protocole

► La fonction *f* est connue de tous.

Propriétés

Problématique

S'aider des mathématiques

Principe

Analogie des couleurs

Faiblesse di protocole

- La fonction f est connue de tous.
- Si on connaît f(x, y) et x alors il est difficile de retrouver y.

Principe

Analogie des couleurs

Faiblesse du protocole

- ▶ La fonction *f* est connue de tous.
- Si on connaît f(x, y) et x alors il est difficile de retrouver y.
- Pour tous entiers x, y, z,

$$f(f(x,y),z)=f(f(x,z),y)$$

Chiffrement asymétrique Diffie-Hellman

Problèmatique

aider des athématiques

Principe

Faiblesse du

En pratique la fonction mathématique utilisée utilise les puissances et le modulo.

Alice

Canal non sécurisé

Étape 1

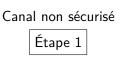
Bob

Chiffrement

asymétrique Diffie-Hellman

Analogie des couleurs

Alice





Bob



Faiblesse

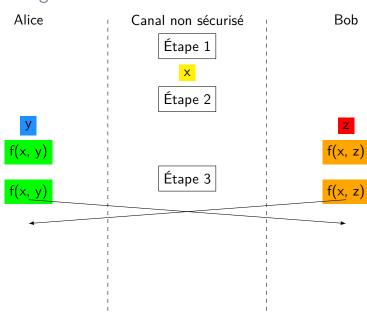
Analogie des couleurs

Chiffrement

asymétrique Diffie-Hellman







Chiffrement asymétrique Diffie-Hellman

Problématique

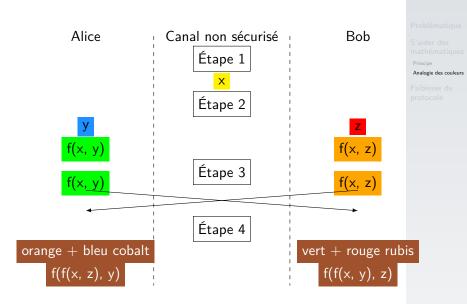
ider des thématiques

Principe

Analogie des couleurs

Faiblesse du protocole





Faiblesse

Chiffrement asymétrique Diffie-Hellman

Problématique

nathématiques

Principe

Analogie des couleurs

Faiblesse du protocole

Il est mathématiquement très difficile pour Eve (eavesdropper : écouteuse) de retrouver les valeurs choisies par Alice et Bob. Cependant, elle n'est pas obligée de le faire.

Alice

Canal non sécurisé

Étape 1

Bob

Chiffrement

asymétrique Diffie-Hellman

Faiblesse du protocole

Alice Canal non sécurisé Étape 1 Étape 2 Eve f(x, y)f(x, y') f(x, z')

Chiffrement asymétrique Diffie-Hellman

Problématique

Bob

f(x, z)

S'aider des mathématiques

Principe

Faiblesse du protocole

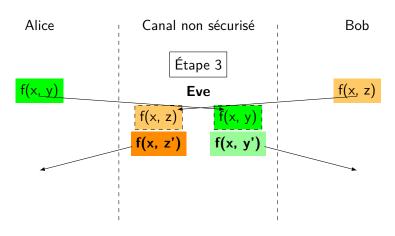


Problématique

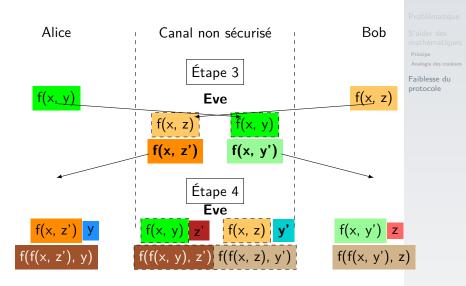
l'aider des nathématiques

Principe Analogie des couleurs

Faiblesse du protocole



Chiffrement asymétrique Diffie-Hellman



Chiffrement asymétrique Diffie-Hellman

Problèmatique

mathématiques

Analogie des couleurs

Faiblesse du protocole

À retenir

Le protocole de Diffie-Hellman permet d'échanger des clés par un canal non sécurisé. Cependant il n'assure pas l'authentification des participants.