

Problématique

S'aider des
mathématiques

Principe
Analogie des couleurs

Faiblesse du
protocole

Chiffrement asymétrique Diffie-Hellman

Christophe Viroulaud

Terminale NSI

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 ?

Problématique

S'aider des
mathématiques

Principe
Analogie des couleurs

Faiblesse du
protocole

Problématique

S'aider des
mathématiques

Principe

Analogie des couleurs

Faiblesse du
protocole

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

Problématique

S'aider des
mathématiques

Principe

Analogie des couleurs

Faiblesse du
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

Problématique

S'aider des
mathématiques

Principe

Analogie des couleurs

Faiblesse du
protocole

- La fonction f est connue de tous.

Problématique

S'aider des
mathématiques

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 .

Problématique

S'aider des
mathématiques

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 ,

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

Problématique

S'aider des
mathématiques

Principe

Analogie des couleurs

Faiblesse du
protocole

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

Analogie des couleurs

Alice

Canal non sécurisé

Bob

Étape 1



Problématique

S'aider des
mathématiques

Principe

Analogie des couleurs

Faiblesse du
protocole

Analogie des couleurs

Alice

y

$f(x, y)$

Canal non sécurisé

Étape 1

x

Étape 2

Bob

z

$f(x, z)$

Problématique

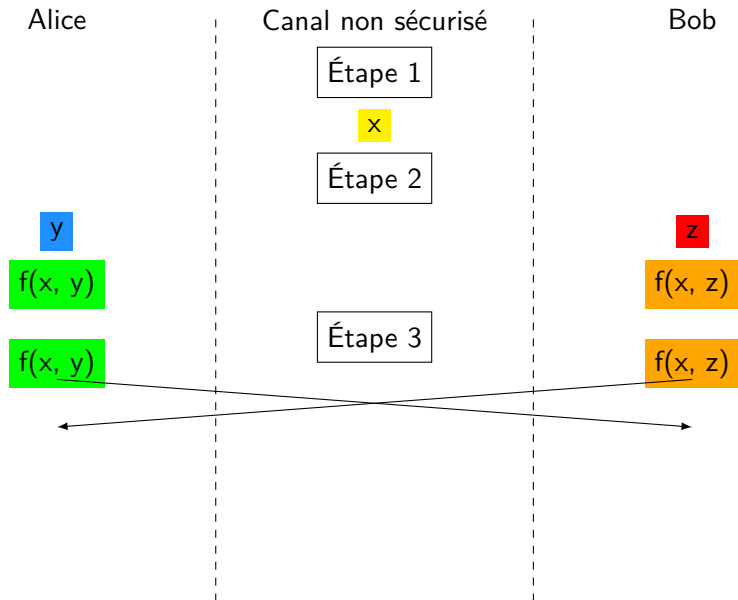
S'aider des
mathématiques

Principe

Analogie des couleurs

Faiblesse du
protocole

Analogie des couleurs



Problématique

S'aider des
mathématiques

Principe
Analogie des couleurs

Faiblesse du
protocole

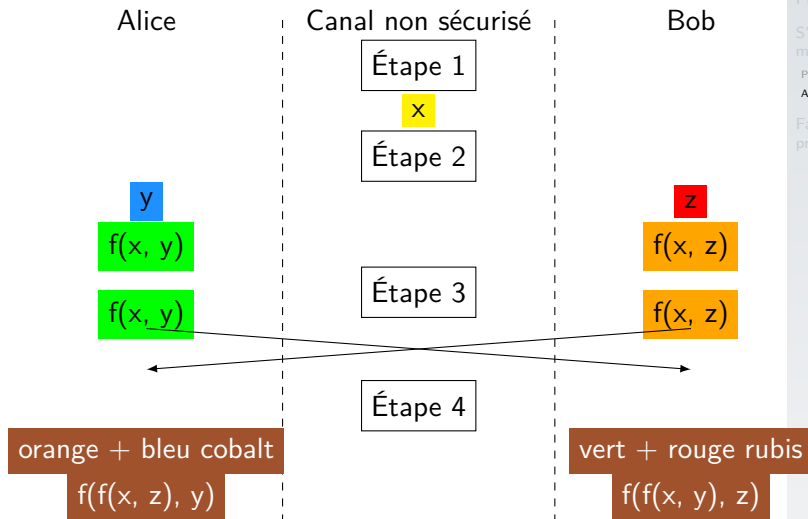
Analogie des couleurs

Problématique

S'aider des
mathématiques

Principe
Analogie des couleurs

Faiblesse du
protocole



Problématique

S'aider des
mathématiques

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.

Man in the middle attack

Alice

Canal non sécurisé

Bob

Étape 1

x

Problématique

S'aider des
mathématiques

Principe

Analogie des couleurs

Faiblesse du
protocole

Man in the middle attack

Alice

y
 $f(x, y)$

Canal non sécurisé

Étape 1

x

Étape 2

Eve

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

Bob

z
 $f(x, z)$

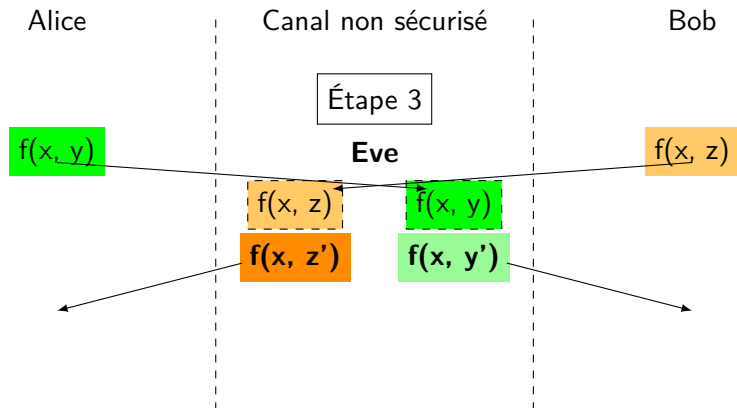
Problématique

S'aider des
mathématiques

Principe
Analogie des couleurs

Faiblesse du
protocole

Man in the middle attack



Problématique

S'aider des
mathématiques

Principe
Analogie des couleurs

Faiblesse du
protocole

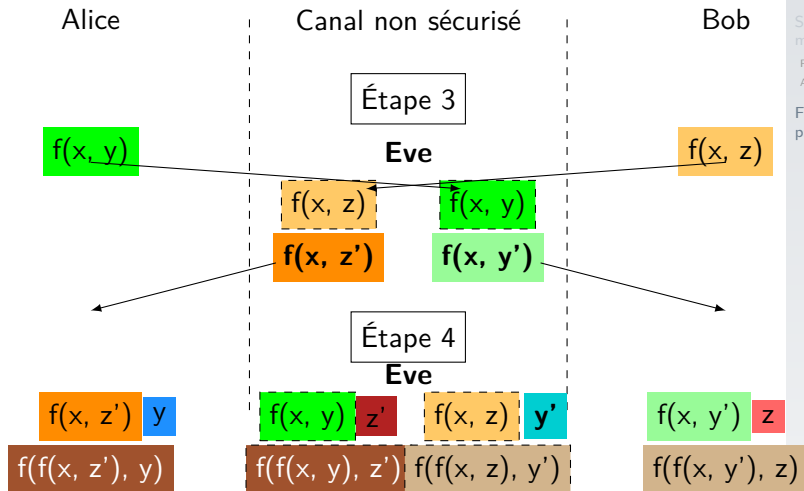
Man in the middle attack

Problématique

S'aider des
mathématiques

Principe
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.