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 ?

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 ?

Les mathématiques à la rescousse
1974 : Le puzzle de Merkle s'appuie sur le coût long du décryptage.

Les mathématiques à la rescousse

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

Les mathématiques à la rescousse
- 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

Les mathématiques à la rescousse

- 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
- La fonction f est connue de tous.

Propriétés

- La fonction f est connue de tous.

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

Propriétés

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

Propriétés
- 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,

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

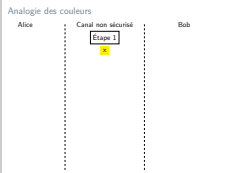
Propriétés

- 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,

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

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

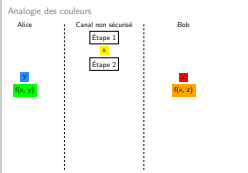
En pratique la fonction mathématique utilisée utilise les puissances et le modulo.



1. Si on connaît jaune et vert il est difficile de retrouver le bleu qui a été utilisé.
2. jaune et la fonction f sont connus de tous. En pratique jaune est un nombre premier (modulo) et f un nombre inférieur (base de la puissance)
   - p = 23
   - f = 5

Analogie des couleurs

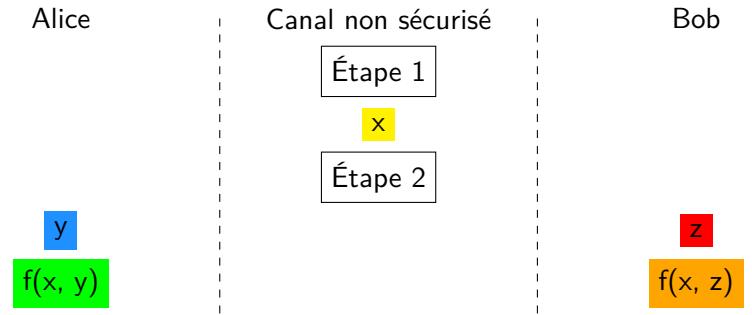
Alice	Canal non sécurisé	Bob
	Étape 1	
	x	

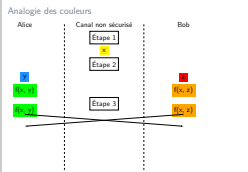


y et z deux nombres : $f^y[mod x]$

- Alice : y $= 6 \rightarrow 5^6[23] = 8$
- Bob : z $= 15 \rightarrow 5^{15}[23] = 19$

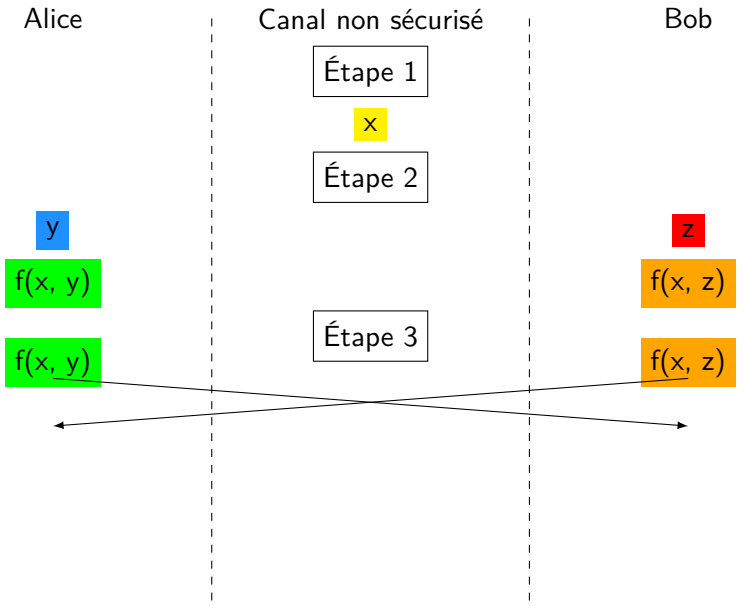
Analogie des couleurs

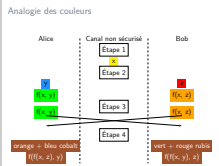




- Alice envoie 8
- Bob envoie 19

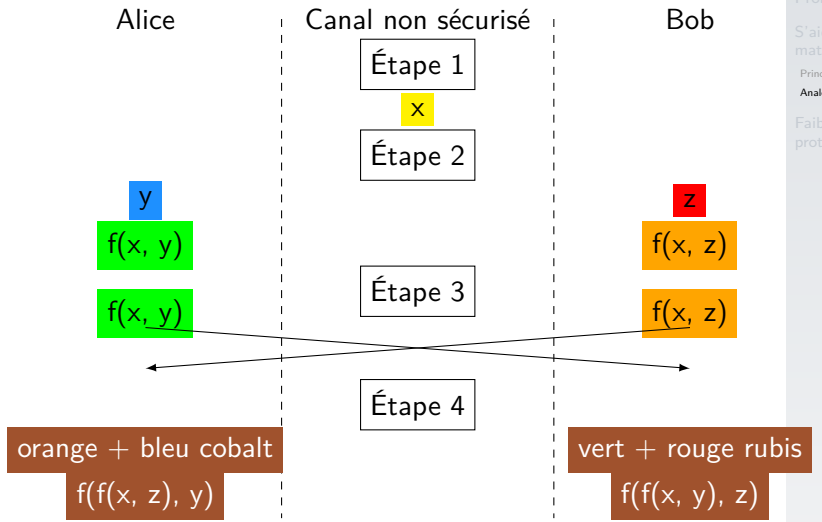
Analogie des couleurs





1. Alice et Bob utilisent le marron comme clé de chiffrement
2. – Alice : $19^6[23] = 2$
   – Bob : $8^{15}[23] = 2$
3. Il faut prendre plus grands nombres pour que brute force ne fonctionne pas.

Analogie des couleurs

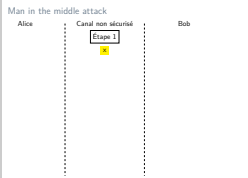


Faiblesse

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.

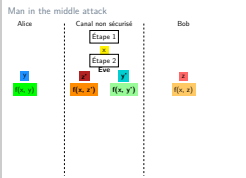
Faiblesse

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.

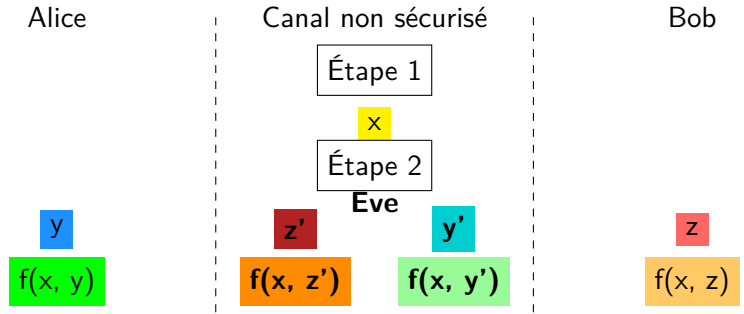


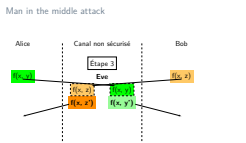
Man in the middle attack

Alice
Canal non sécurisé
Étape 1
x
Bob

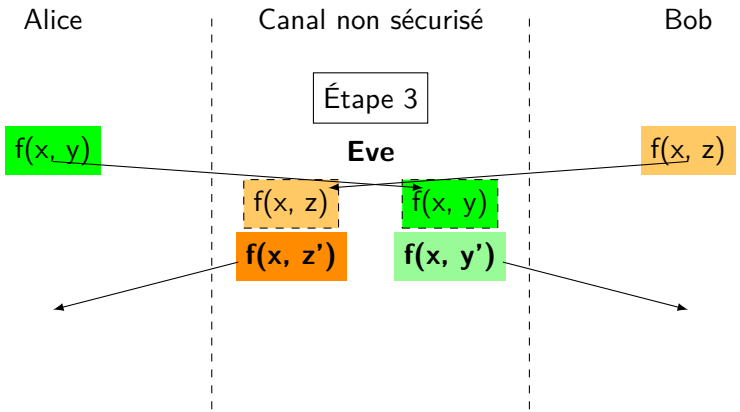


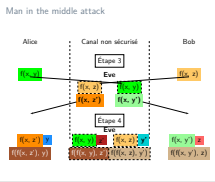
Man in the middle attack



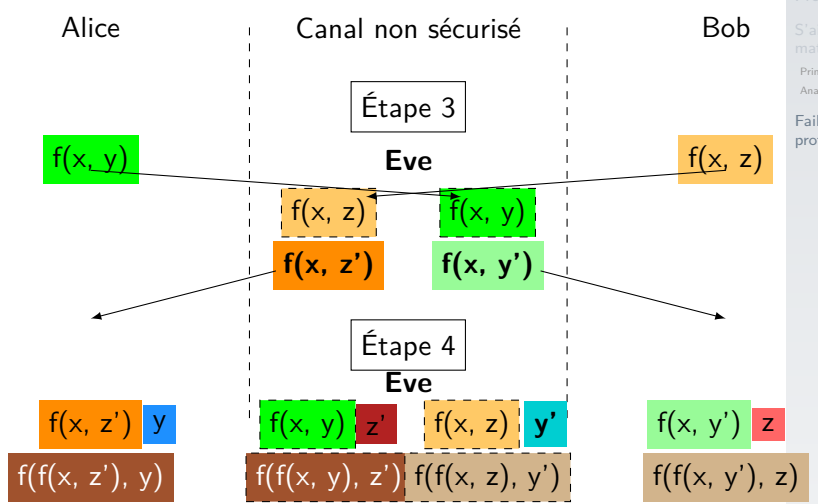


Man in the middle attack





Man in the middle attack



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.

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.