

Chiffrement asymétrique de Diffie-Hellman

Christophe Viroulaud

Terminale - NSI

Archi 22

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.



S'aider des
mathématiques

Principe
Analogie des couleurs
Formalisme mathématique

Faiblesse du
protocole

Eve
Man in the middle attack

S'aider des
mathématiques

Principe

Analogie des couleurs

Formalisme mathématique

Faiblesse du
protocole

Eve

Man in the middle attack

Peut-on échanger une clé de manière sécurisée ?

1. S'aider des mathématiques

1.1 Principe

1.2 Analogie des couleurs

1.3 Formalisme mathématique

2. Faiblesse du protocole

S'aider des mathématiques

Principe

Analogie des couleurs

Formalisme mathématique

Faiblesse du protocole

Eve

Man in the middle attack

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

S'aider des
mathématiques

Principe

Analogie des couleurs

Formalisme mathématique

Faiblesse du
protocole

Eve

Man in the middle attack

S'aider des mathématiques

- ▶ 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.



FIGURE 1 – Prix Turing 2015 : Whitfield Diffie et Martin Hellman

S'aider des
mathématiques

Principe

Analogie des couleurs

Formalisme mathématique

Faiblesse du
protocole

Eve

Man in the middle attack

S'aider des
mathématiques

Principe

Analogie des couleurs

Formalisme mathématique

Faiblesse du
protocole

Eve

Man in the middle attack

- La fonction f est connue de tous.

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

- ▶ 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 ,

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

S'aider des
mathématiques

Principe

Analogie des couleurs

Formalisme mathématique

Faiblesse du
protocole

Eve

Man in the middle attack

À retenir

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

1. S'aider des mathématiques

1.1 Principe

1.2 Analogie des couleurs

1.3 Formalisme mathématique

2. Faiblesse du protocole

S'aider des
mathématiques

Principe

Analogie des couleurs

Formalisme mathématique

Faiblesse du
protocole

Eve

Man in the middle attack

Observation

Classiquement la méthode de Diffie-Hellman est présentée par une analogie de mélanges de couleurs.

Alice

Canal non sécurisé

Bob

Étape 1

x

FIGURE 2 – **clé publique** : une couleur commune est choisie.

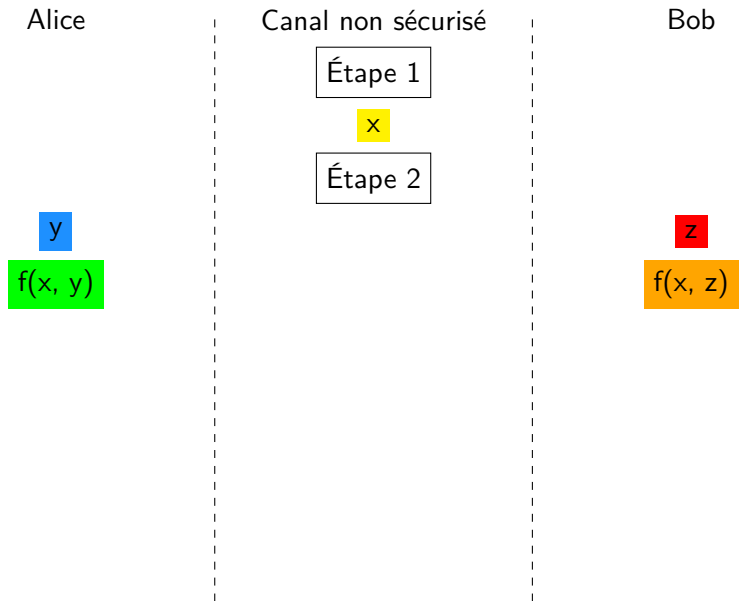


FIGURE 3 – **Clé privée** : chaque individu choisie une couleur et la *mélange* avec la couleur commune.

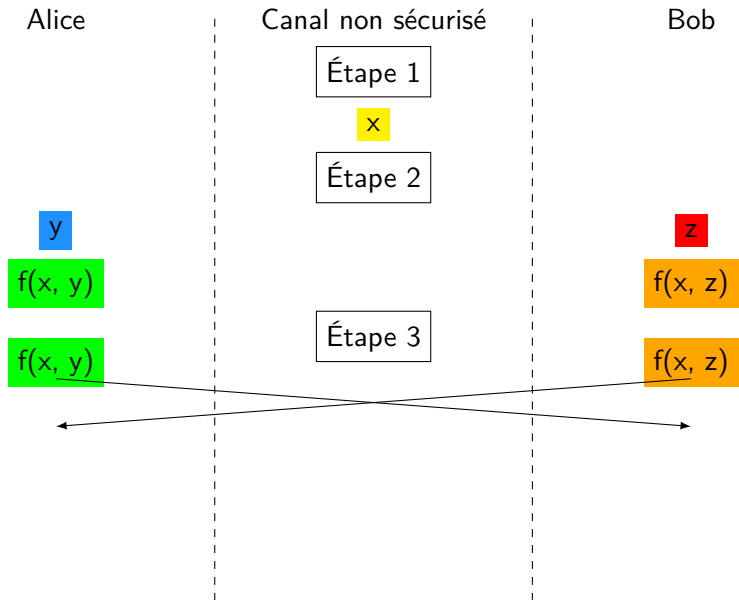


FIGURE 4 – Chaque individu partage sa couleur.

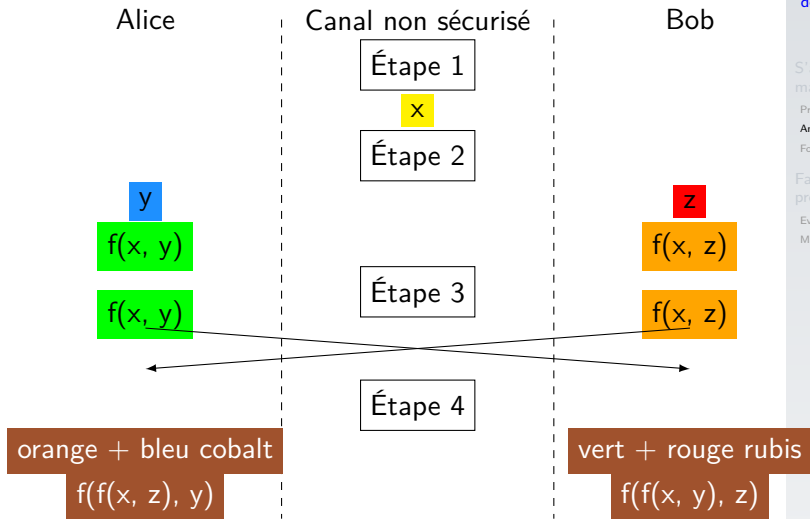


FIGURE 5 – Chaque individu mélange la couleur reçue avec la couleur privée.

Observation

Alice et Bob utilisent le (même) marron comme clé de chiffrement.

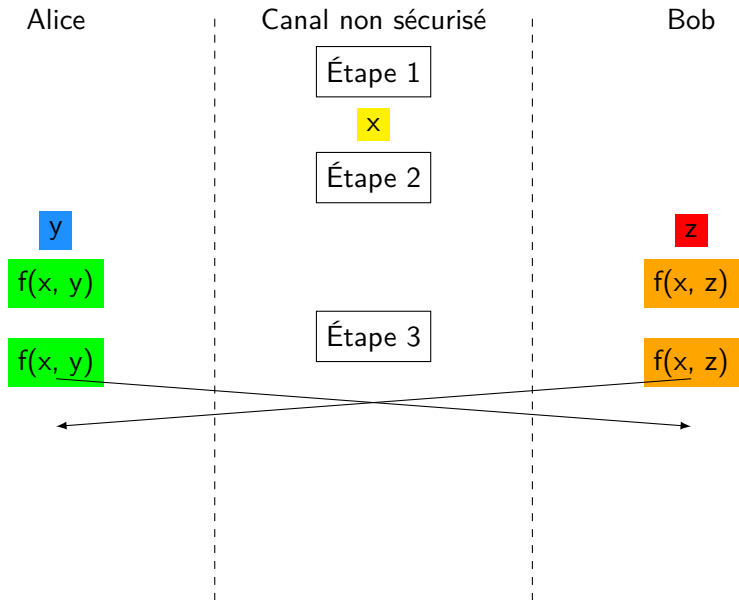


FIGURE 6 – Chaque individu partage sa couleur.

1. S'aider des mathématiques
 - 1.1 Principe
 - 1.2 Analogie des couleurs
 - 1.3 Formalisme mathématique

2. Faiblesse du protocole

S'aider des
mathématiques

Principe

Analogie des couleurs

Formalisme mathématique

Faiblesse du
protocole

Eve

Man in the middle attack

Formalisme mathématique

Alice

Canal non sécurisé

Bob

Étape 1

$$23 \quad f = 5^y \pmod{x}$$

S'aider des
mathématiques

Principe

Analogie des couleurs

Formalisme mathématique

Faiblesse du
protocole

Eve

Man in the middle attack

FIGURE 7 – **clé publique** : une couleur commune est choisie.

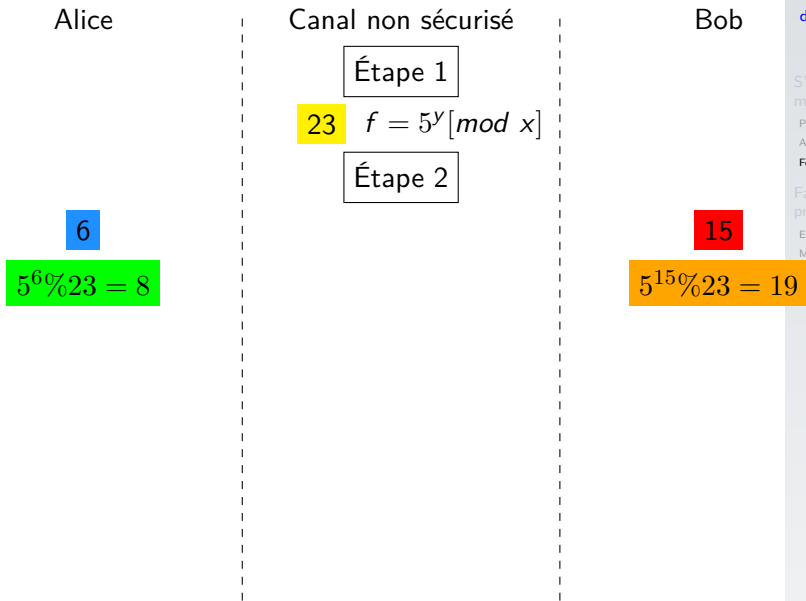


FIGURE 8 – **Clé privée** : chaque individu choisie une couleur et la *mélange* avec la couleur commune.

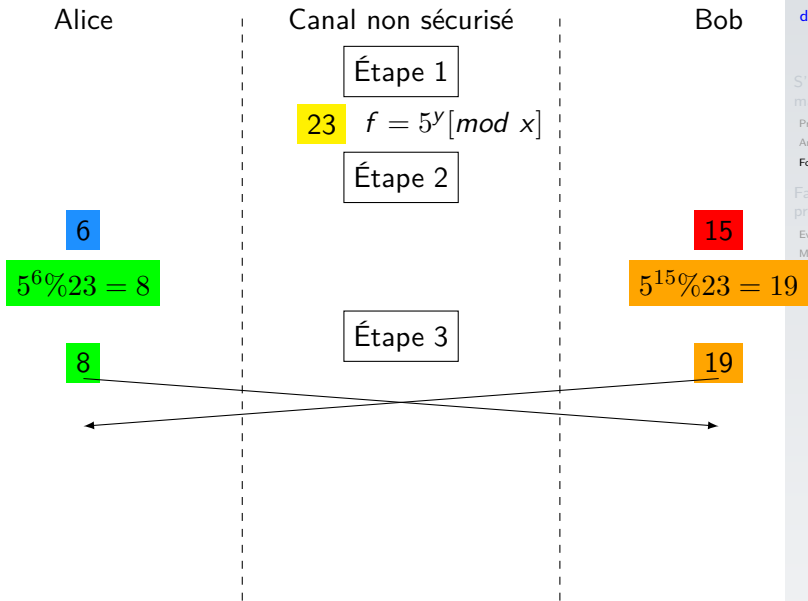


FIGURE 9 – Chaque individu partage sa couleur.

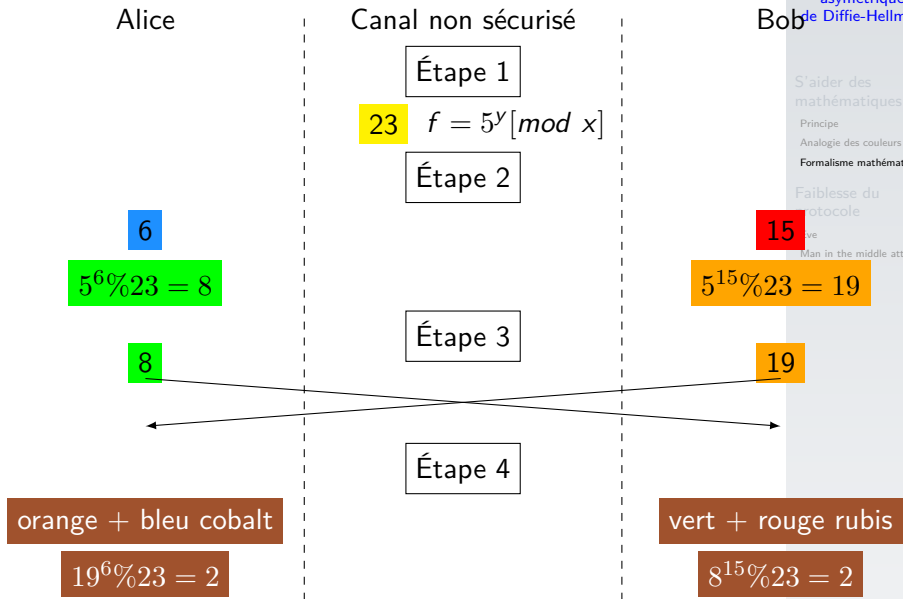


FIGURE 10 – Chaque individu mélange la couleur reçue avec la couleur privée.

À retenir

En pratique on utilise des nombres très grands afin qu'une attaque par force brute ne soit pas efficace.

S'aider des mathématiques

Principe
Analogie des couleurs
Formalisme mathématique

Faiblesse du protocole

Eve
Man in the middle attack

1. S'aider des mathématiques

2. Faiblesse du protocole

2.1 Eve

2.2 Man in the middle attack

Dans la démonstration, Eve est un personnage qui tente de décrypter le message.

À retenir

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

S'aider des
mathématiques

Principe
Analogie des couleurs
Formalisme mathématique

Faiblesse du
protocole

Eve
Man in the middle attack

1. S'aider des mathématiques

2. Faiblesse du protocole

2.1 Eve

2.2 Man in the middle attack

Man in the middle attack

Alice

Canal non sécurisé

Bob

Étape 1

x

Chiffrement
asymétrique
de Diffie-Hellman

S'aider des
mathématiques

Principe
Analogie des couleurs
Formalisme mathématique

Faiblesse du
protocole

Eve
Man in the middle attack

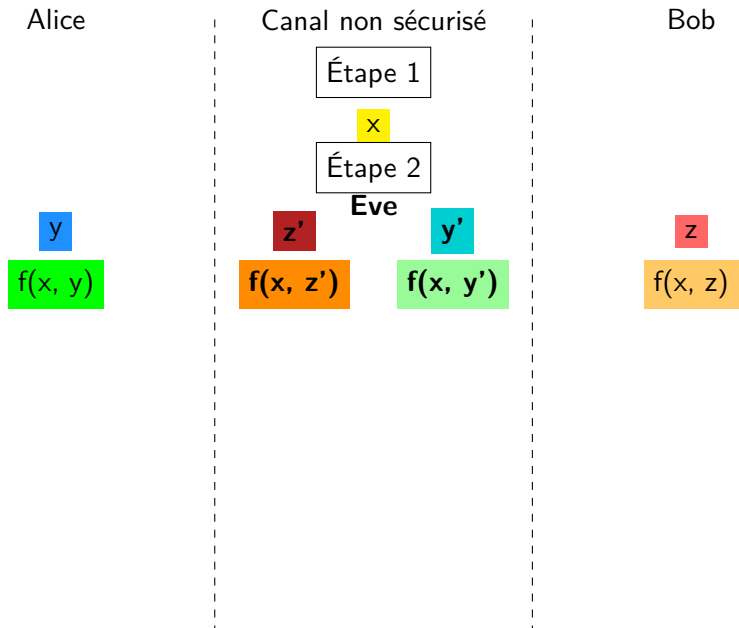


FIGURE 11 – Eve se fait passer pour le destinataire de chaque individu.

Man in the middle attack

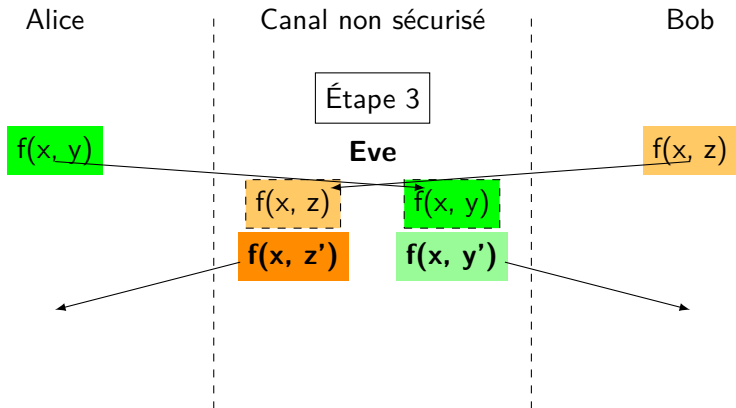


FIGURE 12 – Il n'est pas possible pour Alice et Bob d'être sûr de communiquer avec la bonne personne.

Man in the middle attack

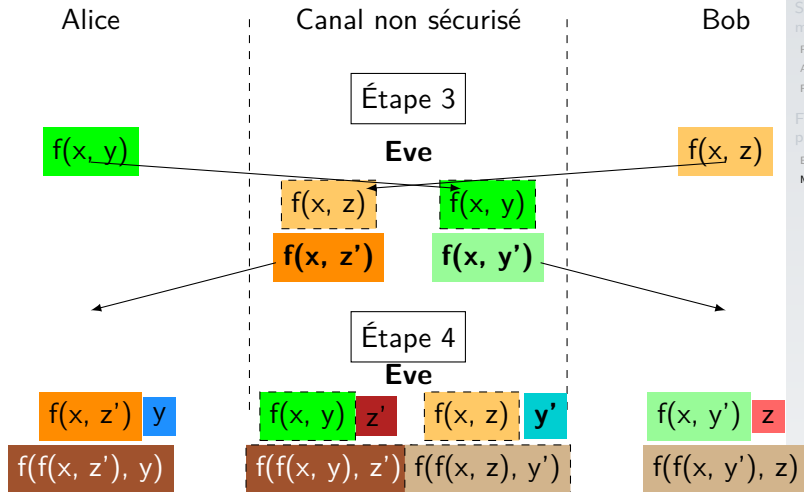


FIGURE 13 – Eve produit des clés pour chaque destinataire.

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.