

Chiffrement asymétrique
de Diffie-Hellman

Christophe Viroulaud

Terminale - NSI

Archi 22

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.



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 ?

Peut-on échanger une clé de manière sécurisée ?

Sommaire

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

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

Chiffrement asymétrique de Diffie-Hellman

S'aider des mathématiques

Principe

S'aider des mathématiques

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

- 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

► 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 .

► 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 ,

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

- 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 ,

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

À retenir

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

À retenir

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

Sommaire

1. S'aider des mathématiques

1.1 Principe

1.2 Analogie des couleurs

1.3 Formalisme mathématique

2. Faiblesse du protocole

Chiffrement asymétrique de Diffie-Hellman

- └ S'aider des mathématiques

- └ Analogie des couleurs

- └ Analogie des couleurs

Analogie des couleurs

Observation

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

Analogie des couleurs

Observation

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

Chiffrement
asymétrique
de Diffie-Hellman

S'aider des
mathématiques

Principe

Analogie des couleurs

Formalisme mathématique

Faiblesse du
protocole

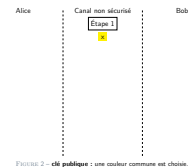
Eve

Man in the middle attack

Chiffrement asymétrique de Diffie-Hellman

- └ S'aider des mathématiques
- └ Analogie des couleurs

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)
 - $p = 23$
 - $f = 5$



Alice

Canal non sécurisé

Bob

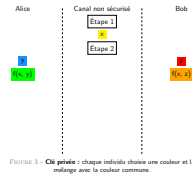
Étape 1

x

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

Chiffrement asymétrique de Diffie-Hellman

- S'aider des mathématiques
- Analogie des couleurs



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

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

Alice

y

f(x, y)

Canal non sécurisé

Étape 1

x

Étape 2

Bob

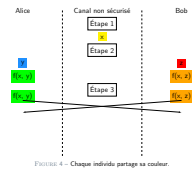
z

f(x, z)

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

Chiffrement asymétrique de Diffie-Hellman

- S'aider des mathématiques
- Analogie des couleurs



- Alice envoie 8
- Bob envoie 19

Alice

Canal non sécurisé

Bob

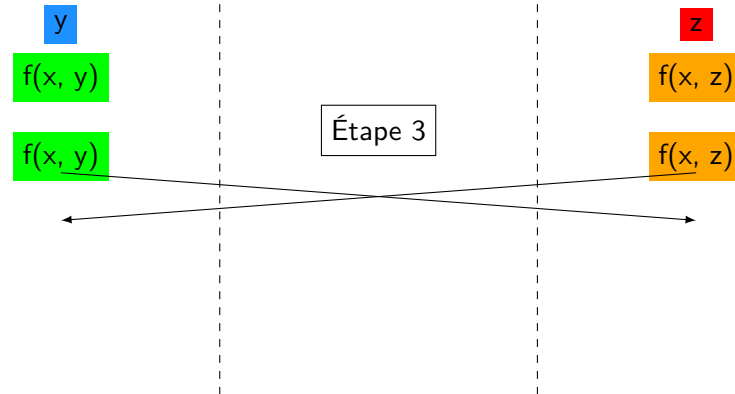
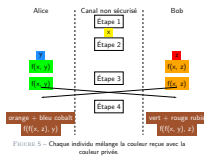


FIGURE 4 – Chaque individu partage sa couleur.

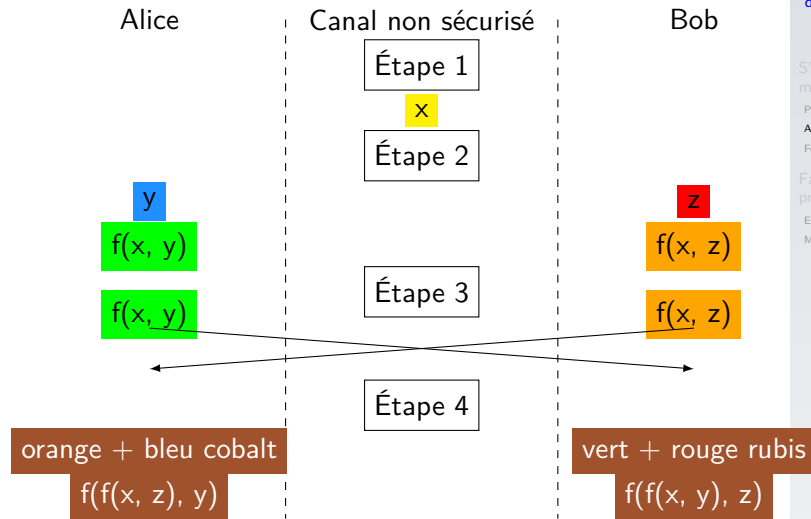
Chiffrement asymétrique de Diffie-Hellman

S'aider des mathématiques

Analogie des couleurs



- Alice : $19^6[23] = 2$
 - Bob : $8^{15}[23] = 2$
- Il faut prendre plus grands nombres pour que brute force ne fonctionne pas.



Observation

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

Observation

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

Sommaire

1. S'aider des mathématiques

1.1 Principe

1.2 Analogie des couleurs

1.3 Formalisme mathématique

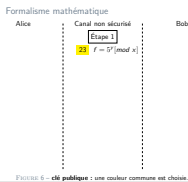
2. Faiblesse du protocole

Chiffrement asymétrique de Diffie-Hellman

- S'aider des mathématiques

- Formalisme mathématique

- Formalisme mathématique



Formalisme mathématique

Alice

Canal non sécurisé

Bob

Étape 1

$$23 \quad f = 5^7 [mod\ x]$$

FIGURE 6 – clé publique : une couleur commune est choisie.

Chiffrement asymétrique de Diffie-Hellman

S'aider des mathématiques

Formalisme mathématique

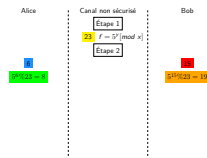


FIGURE 7 – Clé privée : chaque individu choisie une couleur et la mélange avec la couleur commune.

Alice

6

$$5^6 \% 23 = 8$$

Canal non sécurisé

Étape 1

$$23 \quad f = 5^y [mod x]$$

Étape 2

Bob

15

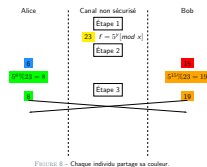
$$5^{15} \% 23 = 19$$

FIGURE 7 – Clé privée : chaque individu choisie une couleur et la mélange avec la couleur commune.

Chiffrement asymétrique de Diffie-Hellman

S'aider des mathématiques

Formalisme mathématique



Alice

Canal non sécurisé

Bob

Étape 1

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

Étape 2

Étape 3

6

$$5^6 \% 23 = 8$$

8

15

$$5^{15} \% 23 = 19$$

19

FIGURE 8 – Chaque individu partage sa couleur.

Chiffrement asymétrique de Diffie-Hellman

S'aider des mathématiques

Formalisme mathématique

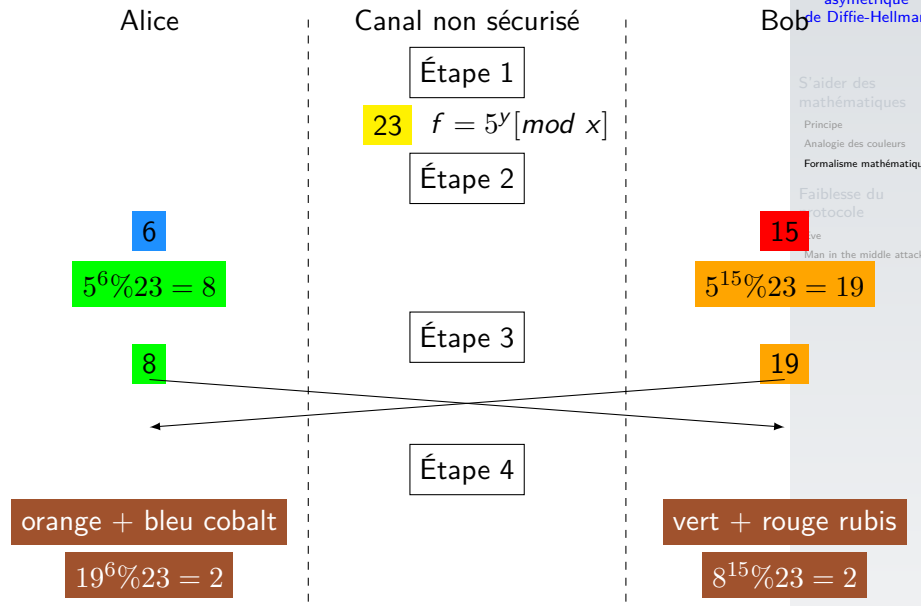
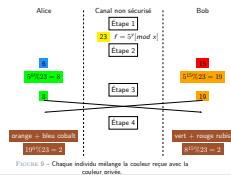


FIGURE 9 – Chaque individu mélange la couleur reçue avec la couleur privée.

À retenir

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

À retenir

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

Sommaire

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 : écouteuse) de retrouver les valeurs choisies par Alice et Bob. Cependant, elle n'est pas obligée de le faire.

Faiblesse du protocole - Eve

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

À retenir

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

Chiffrement asymétrique de Diffie-Hellman

└─ Faiblesse du protocole

└─ Man in the middle attack

└─ Sommaire

Sommaire

1. S'aider des mathématiques

2. Faiblesse du protocole

2.1 Eve

2.2 Man in the middle attack

Sommaire

1. S'aider des mathématiques

2. Faiblesse du protocole

2.1 Eve

2.2 Man in the middle attack

S'aider des
mathématiques

Principe

Analogie des couleurs

Formalisme mathématique

Faiblesse du
protocole

Eve

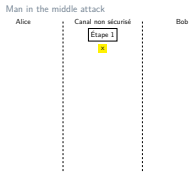
Man in the middle attack

Chiffrement asymétrique de Diffie-Hellman

- Faiblesse du protocole

- Man in the middle attack

- 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

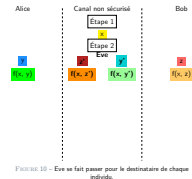
Eve

Man in the middle attack

Chiffrement asymétrique de Diffie-Hellman

Faiblesse du protocole

Man in the middle attack



Alice

y

 $f(x, y)$

Canal non sécurisé

Étape 1

x

Étape 2

Eve

z'

 $f(x, z')$

y'

 $f(x, y')$

Bob

z

 $f(x, z)$

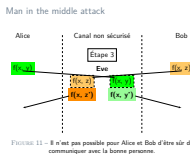
FIGURE 10 – Eve se fait passer pour le destinataire de chaque individu.

Chiffrement asymétrique de Diffie-Hellman

Faiblesse du protocole

Man in the middle attack

Man in the middle attack



Man in the middle attack

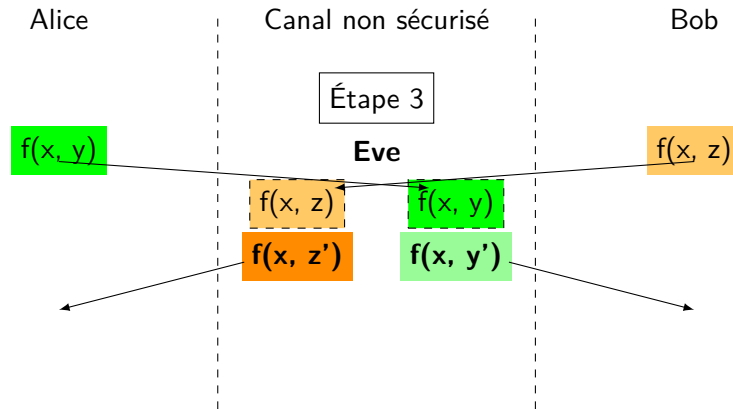


FIGURE 11 – Il n'est pas possible pour Alice et Bob d'être sûr de communiquer avec la bonne personne.

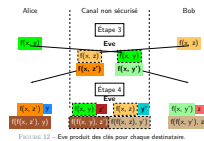
Chiffrement asymétrique de Diffie-Hellman

Faiblesse du protocole

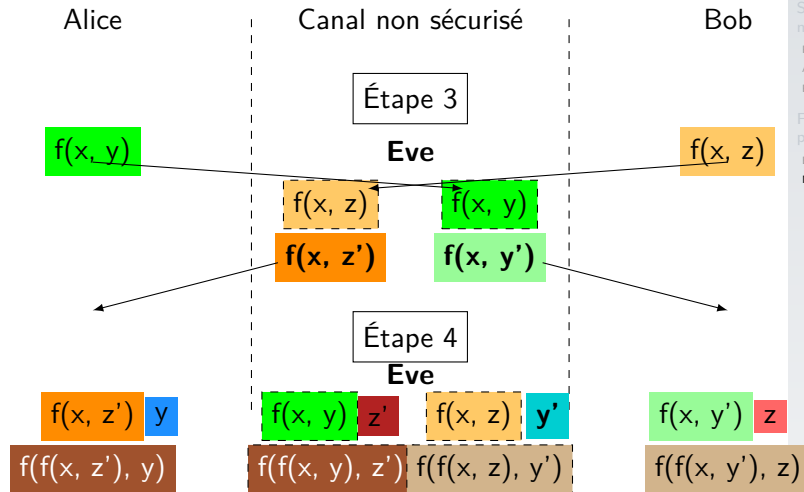
Man in the middle attack

Man in the middle attack

Man in the middle attack



Man in the middle attack



Chiffrement asymétrique de Diffie-Hellman

Faiblesse du protocole

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.