Christophe Viroulaud

Terminale - NSI

Archi 22

Chiffrement asymétrique de Diffie-Hellman

S'aider des mathématiques

1 Illicipe

/ Indiogra des cource

Faiblesse du protocole

Eve

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.



Chiffrement asymétrique de Diffie-Hellman

5'aider des mathématique

Analogie des c

i ormansme matnematiqu

rotocole

ive

S'aider des mathématiques

1 micipe

Analogie des codiedis

Faiblesse dı protocole

ve

Man in the middle attack

Peut-on échanger une clé de manière sécurisée?

S'aider des mathématiques

Principe

Allalogie des codiedis

_ ...

protocole

Eve

- 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

Farmaliana mash (mashimus

Faiblesse di protocole

Eve

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

Chiffrement asymétrique de Diffie-Hellman

S'aider des mathématiques

Principe

Analogie des couleurs

Faiblesse du protocole

Eve

S'aider des mathématiques

Principe

▶ La fonction *f* est connue de tous.

Analogie des cou

Formalisme mathématique

protocole

Eve

S'aider des mathématiques

Principe

Eormalismo mathómatique

-aiblesse du protocole

Eve

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

S'aider des mathématiques

Principe

Formalisme mathématique

rotocole

Eve

- 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.

Chiffrement asymétrique de Diffie-Hellman

S'aider des mathématiques

Principe

Formalisme mathématique

aiblesse di rotocole

ve

Sommaire

Chiffrement asymétrique de Diffie-Hellman

S'aider des mathématiques

Princin

Analogie des couleurs

Formalisme mathématique

protocole

Eve

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

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

Analogie des couleurs

F------

Faiblesse du protocole

ve

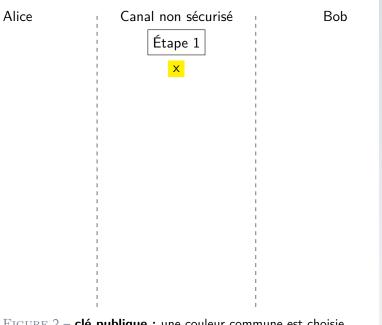
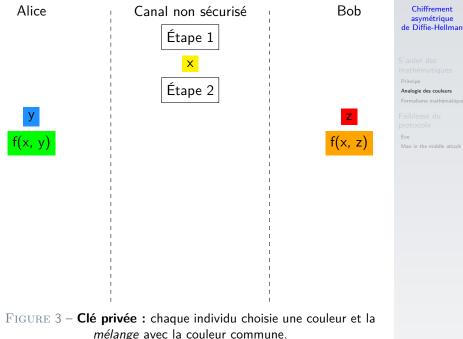


FIGURE 2 – clé publique : une couleur commune est choisie.

Chiffrement

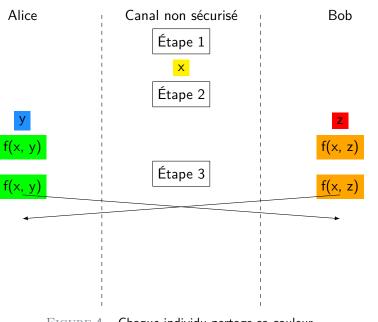
asymétrique de Diffie-Hellman

Analogie des couleurs



mélange avec la couleur commune.

Chiffrement asymétrique



 $\ensuremath{\mathrm{Figure}}$ 4 – Chaque individu partage sa couleur.

Chiffrement

asymétrique de Diffie-Hellman

Analogie des couleurs

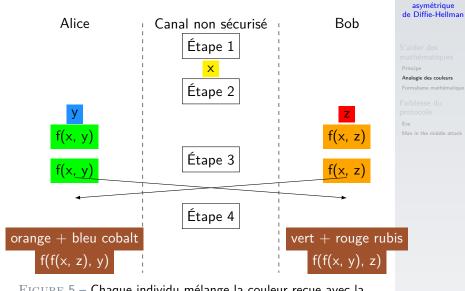


FIGURE 5 – Chaque individu mélange la couleur reçue avec la couleur privée.

Chiffrement

Observation

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

Chiffrement asymétrique de Diffie-Hellman

mathématiques

Analogie des couleurs

Eormalismo mathématique

aiblesse du rotocole

ve

Sommaire

Chiffrement asymétrique de Diffie-Hellman

S'aider des mathématiques

Principe

Analogie des couleur

Formalisme mathématique

protocole

Eve

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

Formalisme mathématique

Alice

Canal non sécurisé

Étape 1

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

Bob

Chiffrement asymétrique de Diffie-Hellman

S'aider des mathématiques

> Principe Analogie des coule

Analogie des couleurs

Formalisme mathématique

Eve

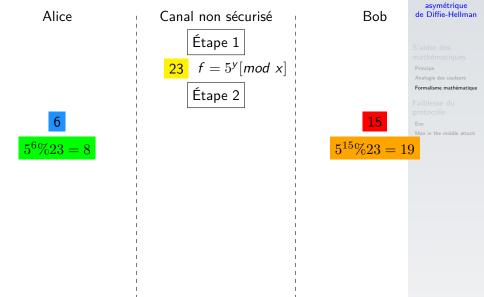
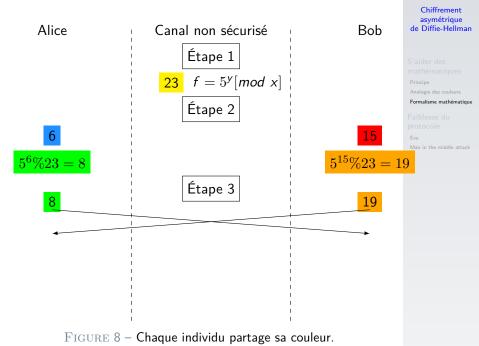


FIGURE 7 – **Clé privée :** chaque individu choisie une couleur et la *mélange* avec la couleur commune.

Chiffrement



18 / 28

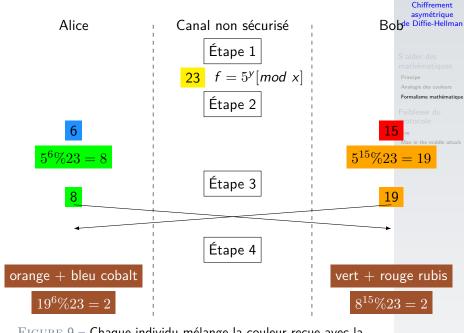


FIGURE 9 – Chaque individu mélange la couleur reçue avec la couleur privée.

À retenir

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

Chiffrement asymétrique de Diffie-Hellman

mathématiques

.

Formalisme mathématique

aiblesse du rotocole

ve

Sommaire

Chiffrement asymétrique de Diffie-Hellman

S'aider des mathématiques

- 2. Faiblesse du protocole
- 2.1 Eve
- 2.2 Man in the middle attack

S'aider des mathématique

Principe

Analogie des couleurs

Faiblesse du

protocole

Eve

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

Chiffrement asymétrique de Diffie-Hellman

mathématiques

Principe

F-----li---- ------li-----

Faiblesse du protocole

Eve

Sommaire

- Chiffrement asymétrique de Diffie-Hellman
- mathématiques
- Analogie des couler
- Formalisme mathématique
- protocole
- Eve

- 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

Étape 1



Bob

Chiffrement

asymétrique de Diffie-Hellman

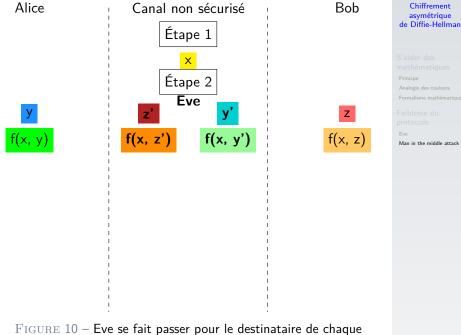


FIGURE 10 – Eve se fait passer pour le destinataire de chaque individu.

Formalisme mathématique

aiblesse du rotocole

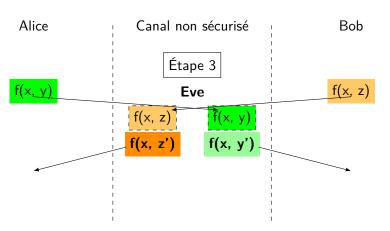


FIGURE 11 – Il n'est pas possible pour Alice et Bob d'être sûr de communiquer avec la bonne personne.

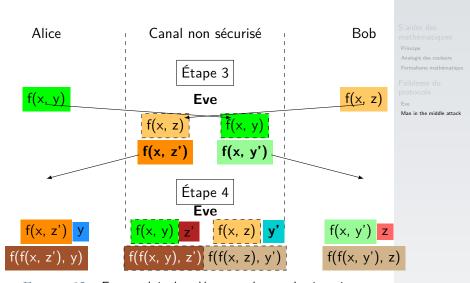


FIGURE 12 – Eve produit des clés pour chaque destinataire.

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.

Chiffrement asymétrique de Diffie-Hellman

o aider des mathématiques

Analogie des couleur

aiblesse du rotocole