Chiffrement asymétriqueDiffie-Hellman

Diffie-Hellman

Christophe Viroulaud

Terminale NSI

Chiffrement asymétrique Diffie-Hellman

Christophe Viroulaud

Terminale NSI

1 / 15

Chiffrement asymétrique Diffie-Hellman

## Chiffrement asymétriqueDiffie-Hellman Problématique

Problématique



#### 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?

Chiffrement asymétrique Diffie-Hellman

Problématique

l'aider des nathématiques

Analogie des couleurs



#### Les mathématiques à la rescousse

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

Chiffrement asymétrique Diffie-Hellman

roblémati

Principe Principe

Principe

Analogie des couleurs

aiblesse du otocole Les mathématiques à la rescousse

► 1974 : Le puzzle de Merkle s'appuie sur le coût long du

Chiffrement asymétrique Diffie-Hellman

Problématique

mathématiques

Principe

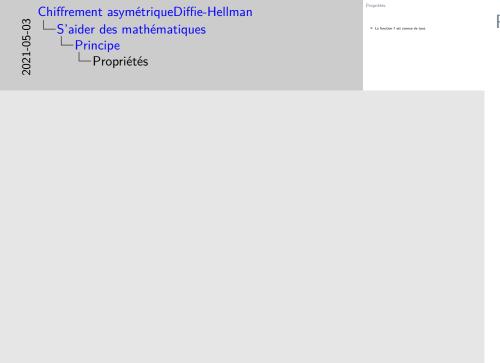
Analogie des couleurs

Analogie des couleurs

rotocole

▶ 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

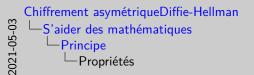
► La fonction *f* est connue de tous.

Chiffrement

asymétrique Diffie-Hellman

Principe

4 / 15



Propriétés

Propriétés

La fonction f est connue de tous. ► Si on connaît f(x, v) et x alors il est difficile de

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

Chiffrement asymétrique Diffie-Hellman

Principe

Propriétés

Propriétés

La fonction f est connue de tous

Pour tous entiers x. v. z.

► Si on connaît f(x, v) et x alors il est difficile de retrouver y.

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

Chiffrement

asymétrique

Diffie-Hellman

Principe

- ▶ La fonction *f* est connue de tous.
- ightharpoonup Si on connaît f(x,y) et x alors il est difficile de retrouver y.
- $\triangleright$  Pour tous entiers x, y, z,

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

biematiqu

mathématiques Principe

Principe Analogie des couleurs

iblesse du otocole

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

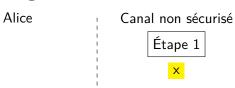
# Chiffrement asymétriqueDiffie-Hellman S'aider des mathématiques Analogie des couleurs Analogie des couleurs

- 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)

$$- p = 23$$

$$- f = 5$$

#### Analogie des couleurs



Bob

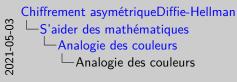


Analogie des couleurs

Chiffrement

asymétrique Diffie-Hellman

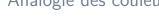
Faiblesse du protocole



f(x, z)

Analogie des couleurs

Analogie des couleurs



Canal non sécurisé

Étape 1

Bob

y et z deux nombres :  $f^y[modx]$ 

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



Alice

Chiffrement

asymétrique Diffie-Hellman

Analogie des couleurs

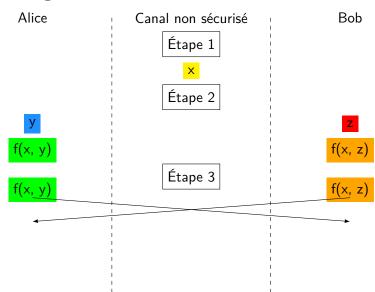
Analogie des couleurs Étape 3

Alice envoie 8

2021-05-03

■ Bob envoie 19

## Analogie des couleurs Alice



Chiffrement

asymétrique Diffie-Hellman

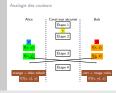
Analogie des couleurs

#### Chiffrement asymétriqueDiffie-Hellman

—S'aider des mathématiques

Analogie des couleurs

Analogie des couleurs

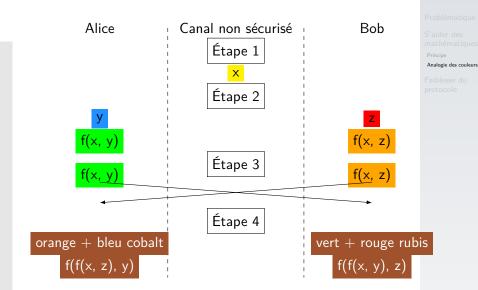


- 1. Alice et Bob utilisent le marron comme clé de chiffrement
- 2. Alice:  $19^6[23] = 2$

- Bob :  $8^{15}[23] = 2$ 

3. Il faut prendre plus grands nombres pour que brute force ne fonctionne pas.

#### Analogie des couleurs



Chiffrement

asymétrique Diffie-Hellman



2021-05-03

#### Faiblesse

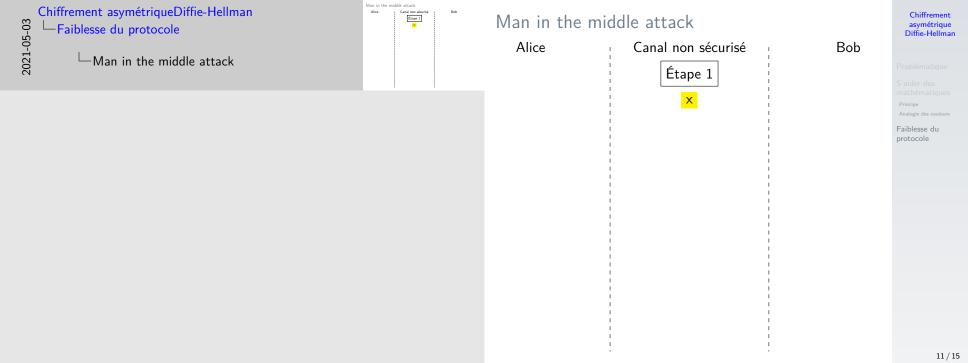
Chiffrement

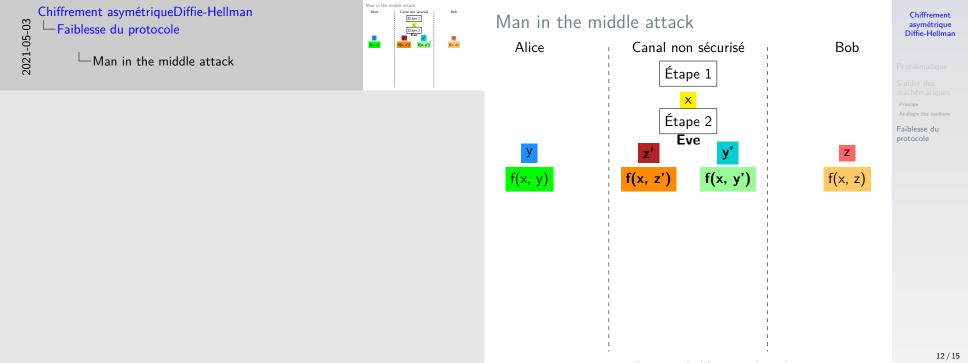
asymétrique

Diffie-Hellman

Faiblesse du protocole

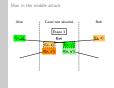
Il est mathématiquement très difficile pour Eve (eavesdropper : écouteuse) de retrouver les valeurs choisies par Alice et Bob. Cependant, elle n'est pas obligée de le faire.



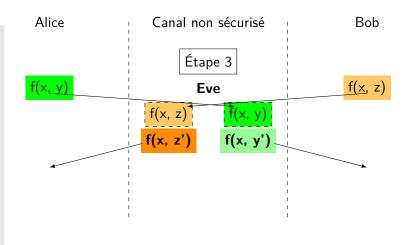


# Chiffrement asymétriqueDiffie-Hellman Faiblesse du protocole

☐ Man in the middle attack



#### Man in the middle attack



Chiffrement asymétrique Diffie-Hellman

Problématique

S'aider des mathématiques Principe

Analogie des couleurs

Faiblesse du protocole

2021-05-03



#### Man in the middle attack

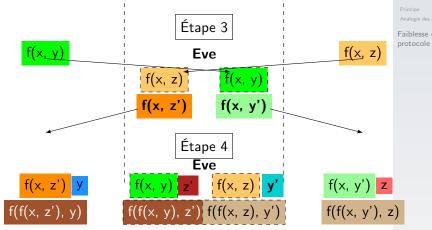
Alice





Bob

Faiblesse du



Canal non sécurisé

#### 

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.

Chiffrement asymétrique Diffie-Hellman

Problématique

'aider des lathématiques

Analogie des couleurs

Faiblesse du protocole