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

Sommaire

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

S'aider des mathématiques

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

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.

- 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

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.

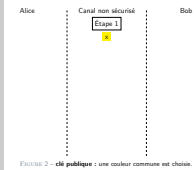


FIGURE 2 – **clé publique :** une couleur commune est choisie.

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

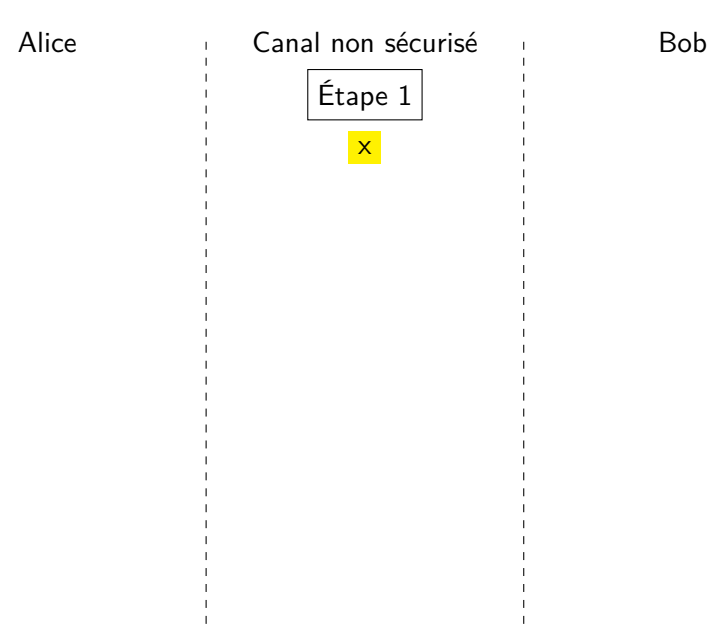


FIGURE 2 – **clé publique :** une couleur commune est choisie.

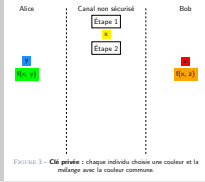


FIGURE 3 – **Clé privée :** chaque individu choisie une couleur et la *mélange* avec la couleur commune.

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

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

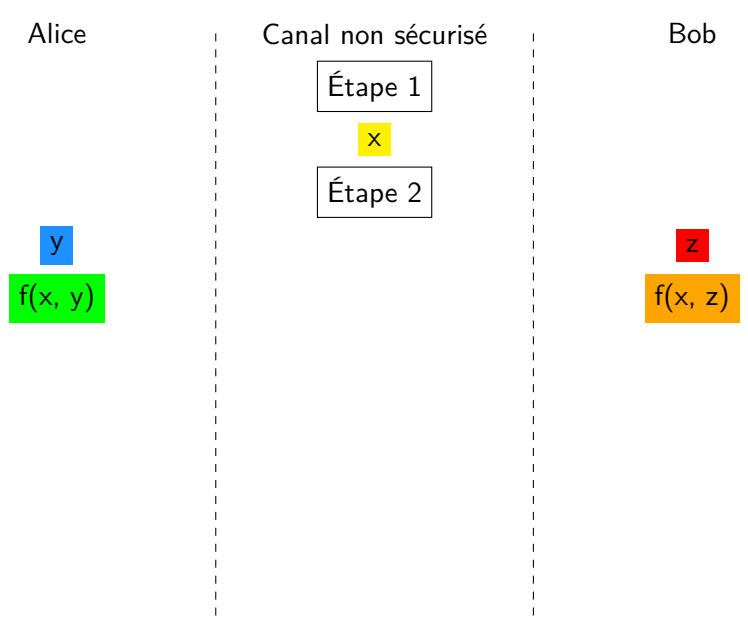


FIGURE 3 – **Clé privée :** chaque individu choisie une couleur et la *mélange* avec la couleur commune.

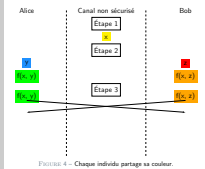


FIGURE 4 – Chaque individu partage sa couleur.

- Alice envoie 8
- Bob envoie 19

Alice
Canal non sécurisé
Bob
Étape 1
x
Étape 2
y
f(x, y)
f(x, y)
Étape 3
z
f(x, z)
f(x, z)
FIGURE 4 – Chaque individu partage sa couleur.

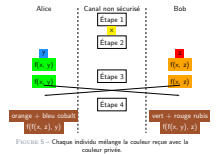


FIGURE 5 – Chaque individu mélange la couleur reçue avec la couleur privée.

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

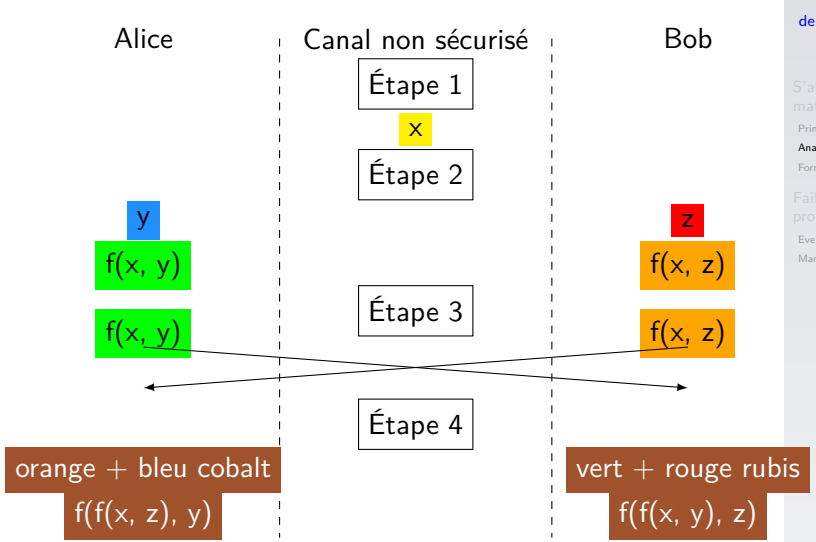


FIGURE 5 – Chaque individu mélange la couleur reçue avec la couleur privée.

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

Observation

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

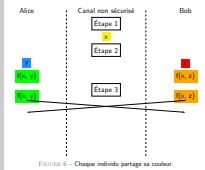


FIGURE 6 – Chaque individu partage sa couleur.

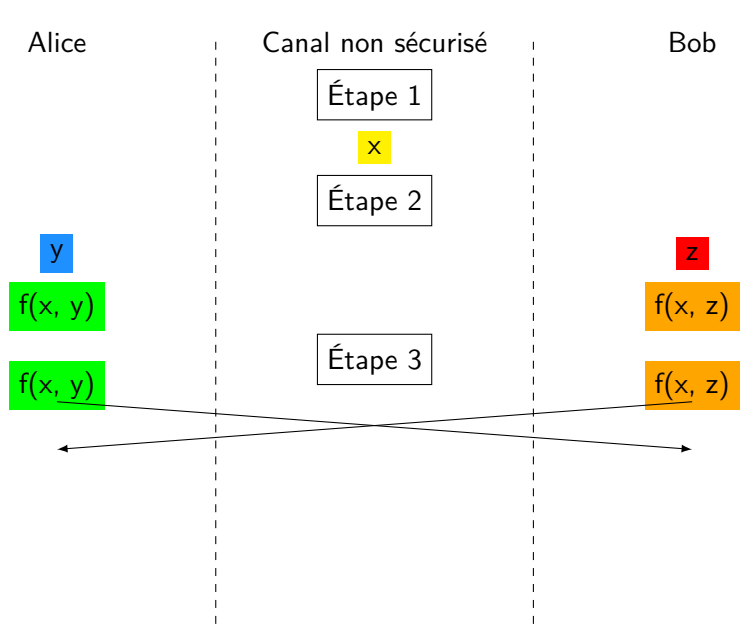


FIGURE 6 – Chaque individu partage sa couleur.

Sommaire

Sommaire

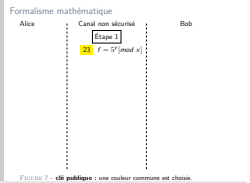


FIGURE 7 – **clé publique :** une couleur commune est choisie.

Formalisme mathématique

Alice	Canal non sécurisé	Bob
	Étape 1	
	23 $f = 5^y [mod\ x]$	

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

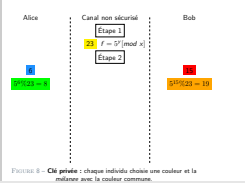


FIGURE 8 – **Clé privée :** chaque individu choisie une couleur et la *mélange* avec la couleur commune.

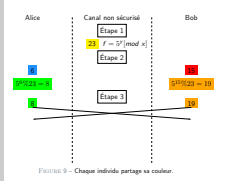


FIGURE 9 – Chaque individu partage sa couleur.

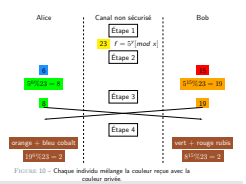


FIGURE 10 – Chaque individu mélange la couleur reçue avec la couleur privée.

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

À retenir

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

Sommaire

Sommaire

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.

Faiblesse du protocole - Eve

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

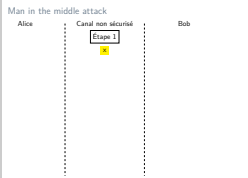
À retenir

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.

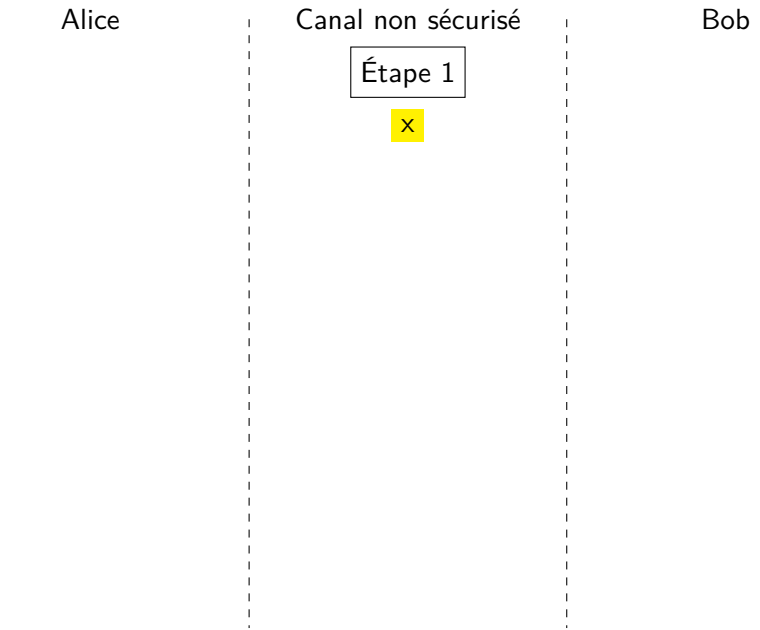
Sommaire

1. S'aider des mathématiques
2. Faiblesse du protocole
2.2 Man in the middle attack

Sommaire



Man in the middle attack



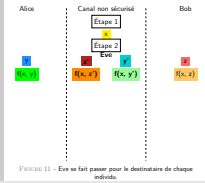


FIGURE 11 – Eve se fait passer pour le destinataire de chaque individu.

Alice
Canal non sécurisé
Bob
Étape 1
x
Étape 2
Eve
y
z'
y'
z
f(x, y)
f(x, z')
f(x, y')
f(x, z)

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

Man in the middle attack

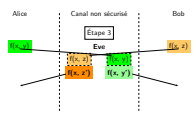


FIGURE 12 – Il n'est pas possible pour Alice et Bob d'être sûr de communiquer avec la bonne personne.

Man in the middle attack

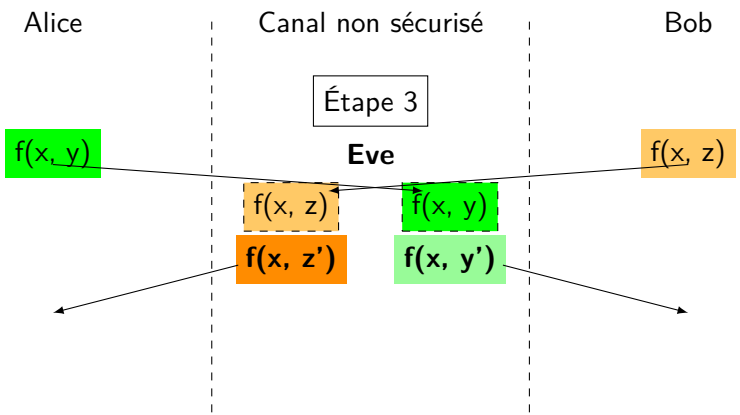


FIGURE 12 – Il n'est pas possible pour Alice et Bob d'être sûr de communiquer avec la bonne personne.

Man in the middle attack

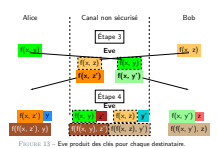


FIGURE 13 – Eve produit des clés pour chaque destinataire.

Man in the middle attack

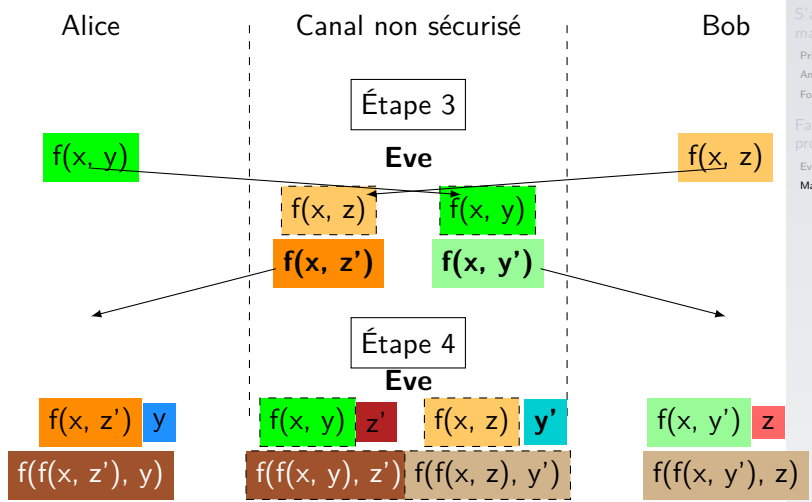


FIGURE 13 – Eve produit des clés pour chaque destinataire.

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.

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.