1 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. La difficulté ici est donc de pouvoir s'échanger cette clé de manière sécurisée.

Peut-on échanger une clé de manière sécurisée ?

2 S'aider des mathématiques

2.1 Principe

Pour résoudre le problème de l'échange de clés **Diffie et Hellman**, deux cryptologues américains, proposent en 1976 une méthode pour convenir d'une clé symétrique partagée en passant par un canal non sécurisé. Cet algorithme s'appuie sur une fonction mathématique, notée *f*, telle que :

— 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, $f(f(x, y), z) = f(f(x, z), y)$

2.2 Analogie des couleurs

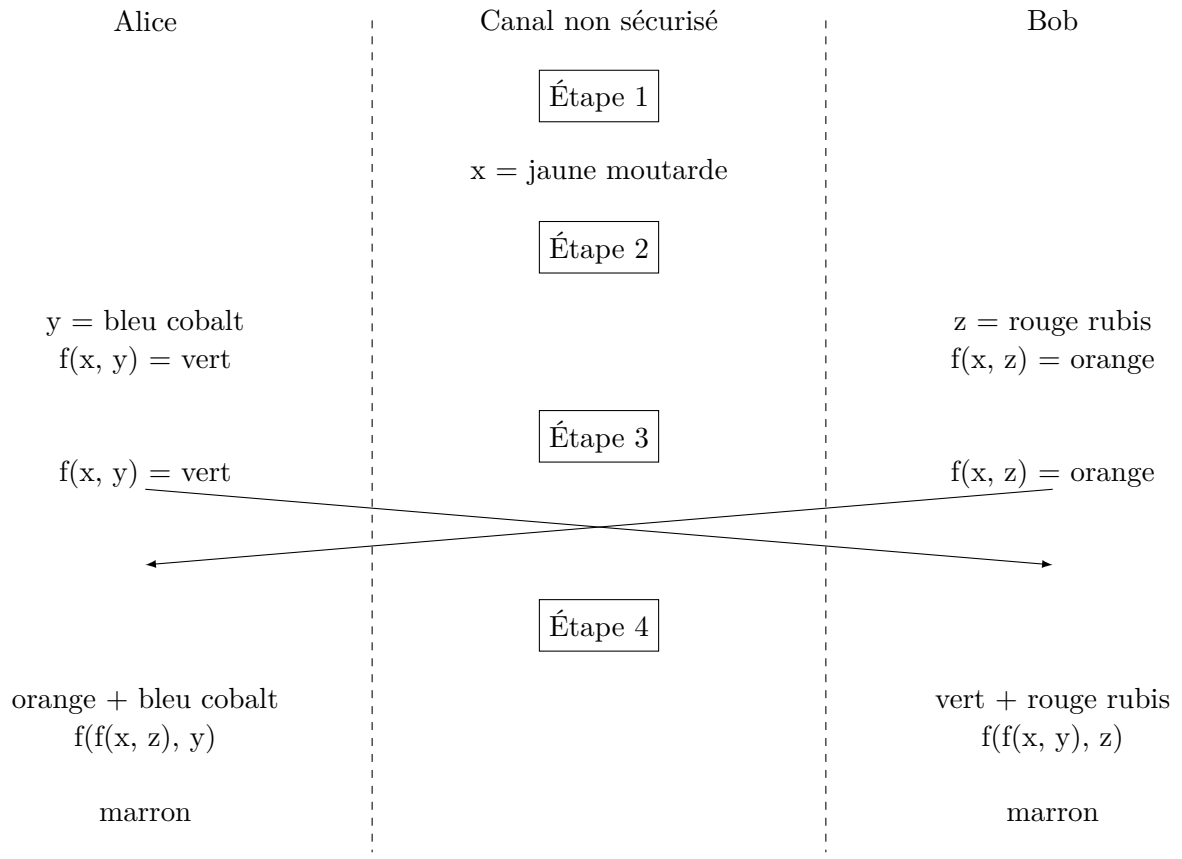

FIGURE 1 – Analogie des couleurs

3 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.

Christophe Viroulaud

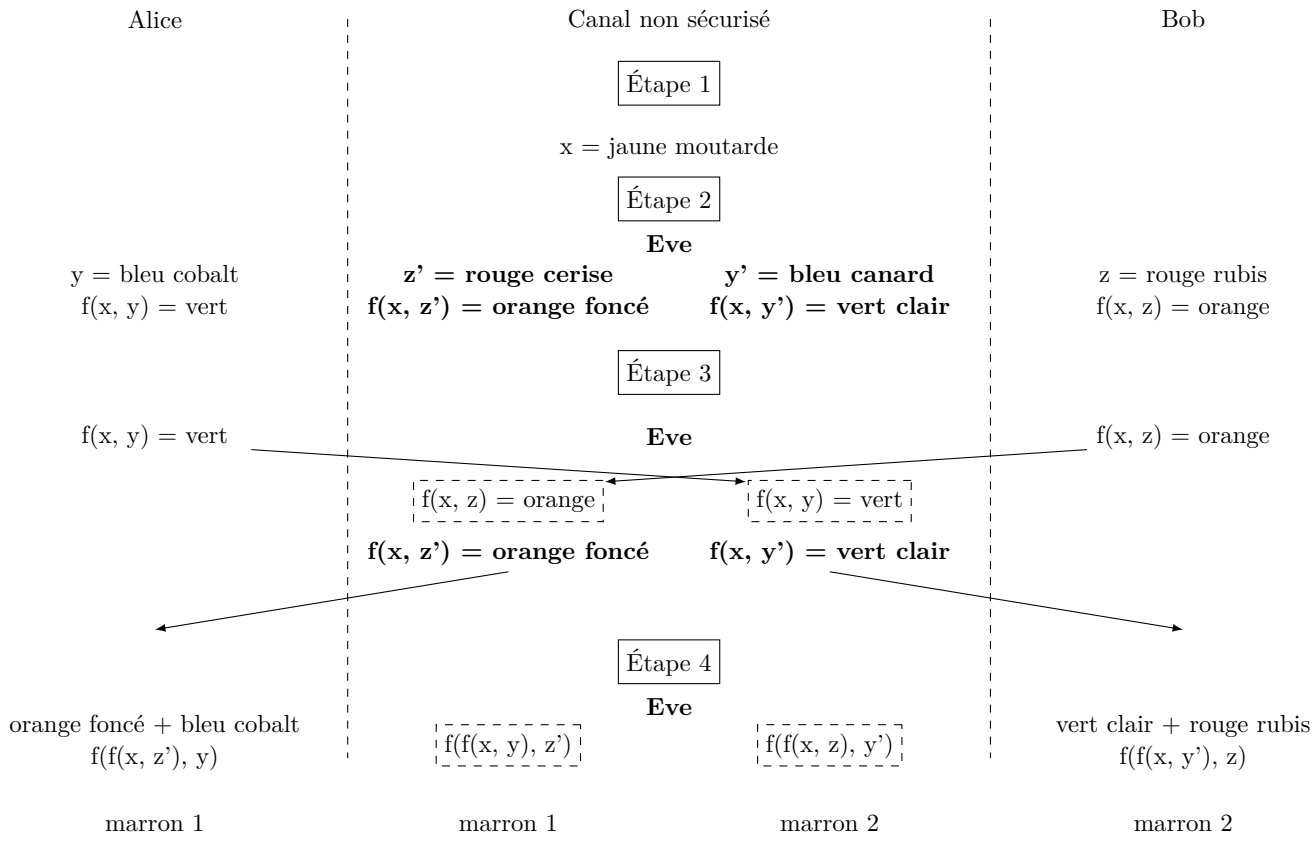

FIGURE 2 – Attaque de l'homme du milieu

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.

Christophe Viroulaud