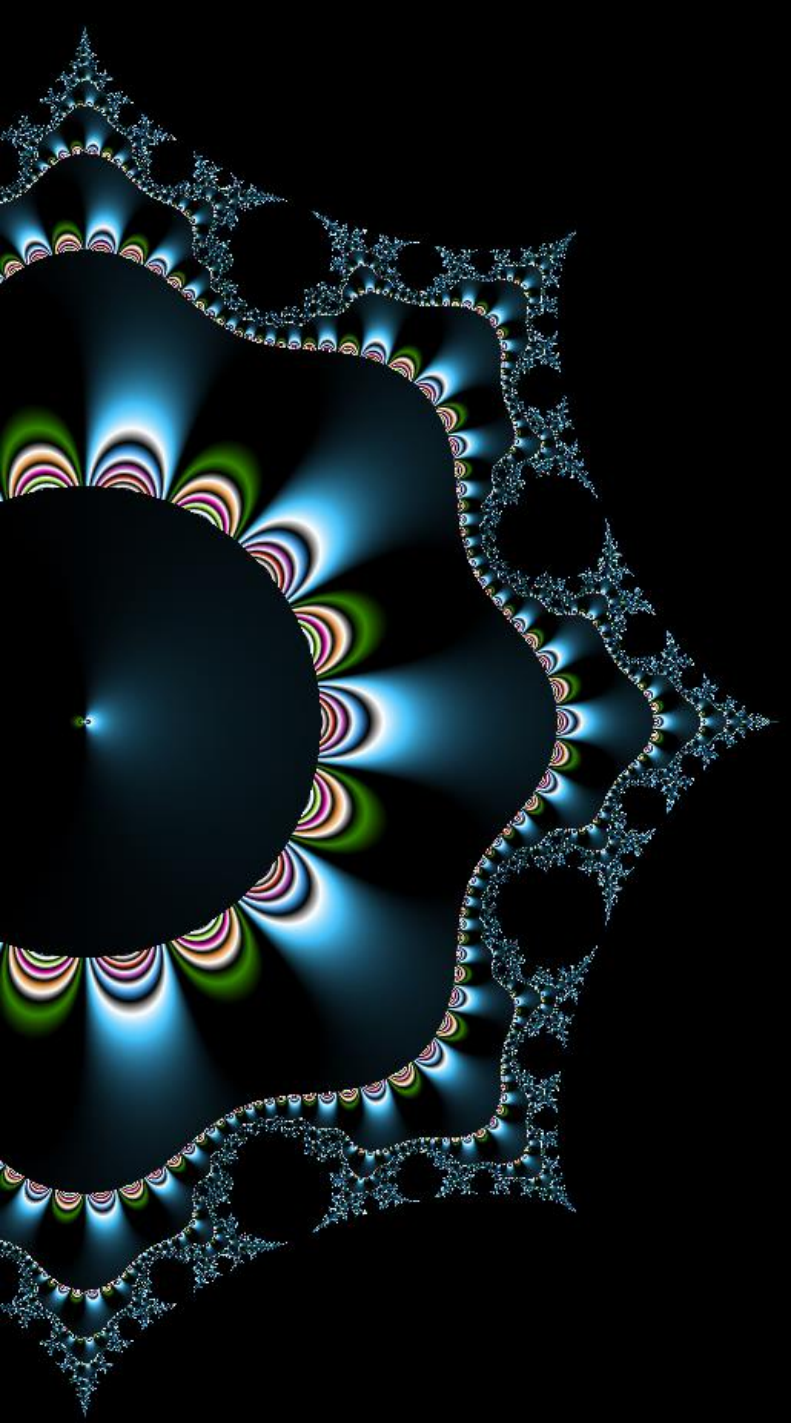


07 Cryptographie

Algorithmes symétriques

Corinne HENIN

www.arsouyes.org

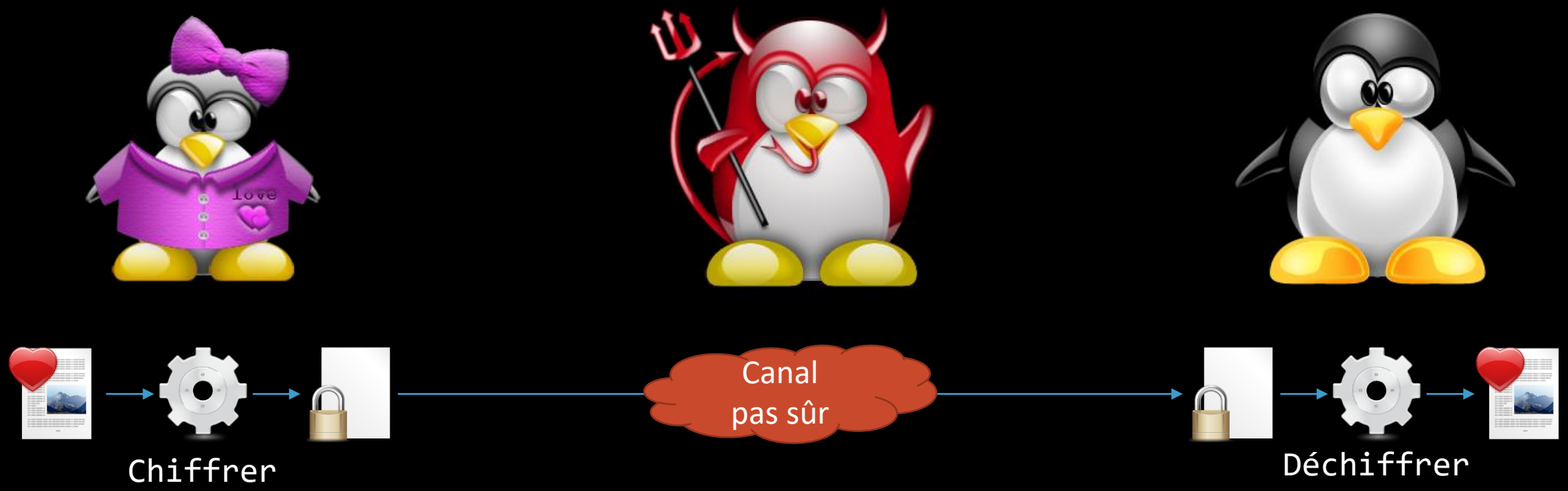
Quel est le problème

Canal de communication non sûr

Eve écoute

Principe de la cryptographie

Eve perd ses pouvoirs



Cryptographie symétrique

Principe

Une clé 🔑

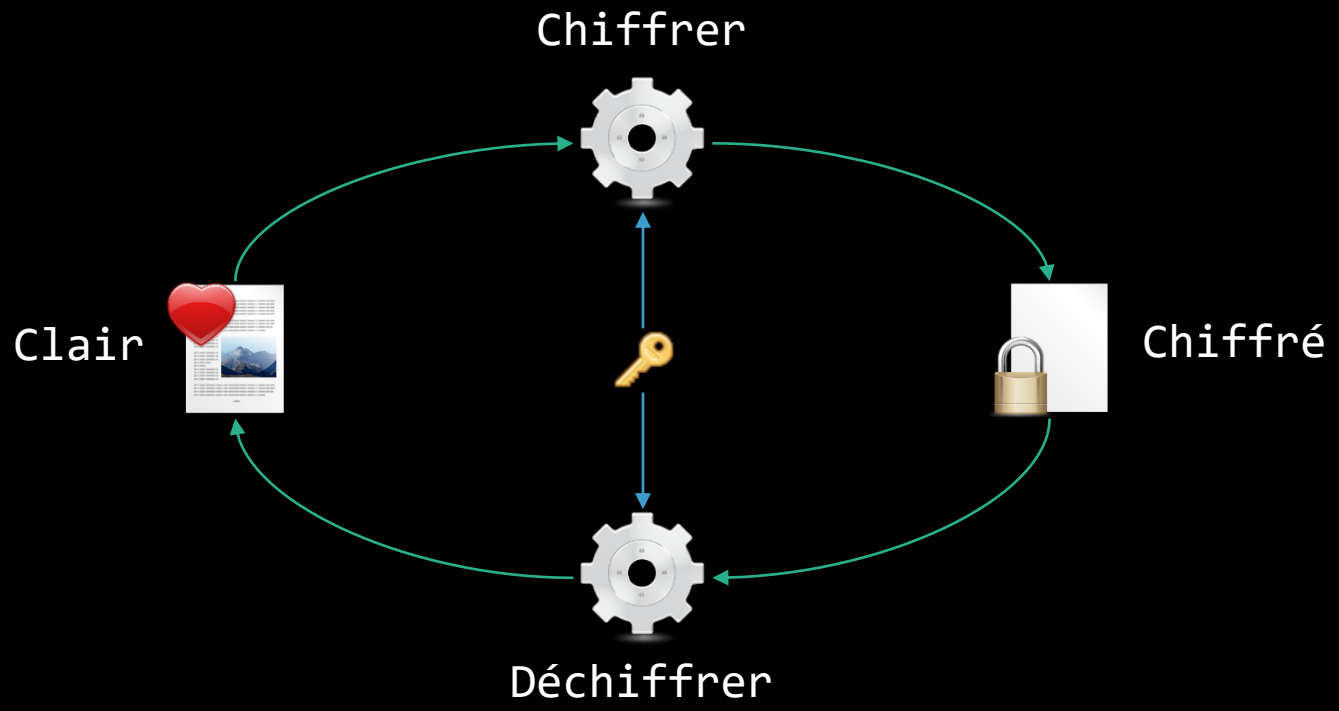
Commune aux correspondants

Chiffre et déchiffre

Annule ses effets

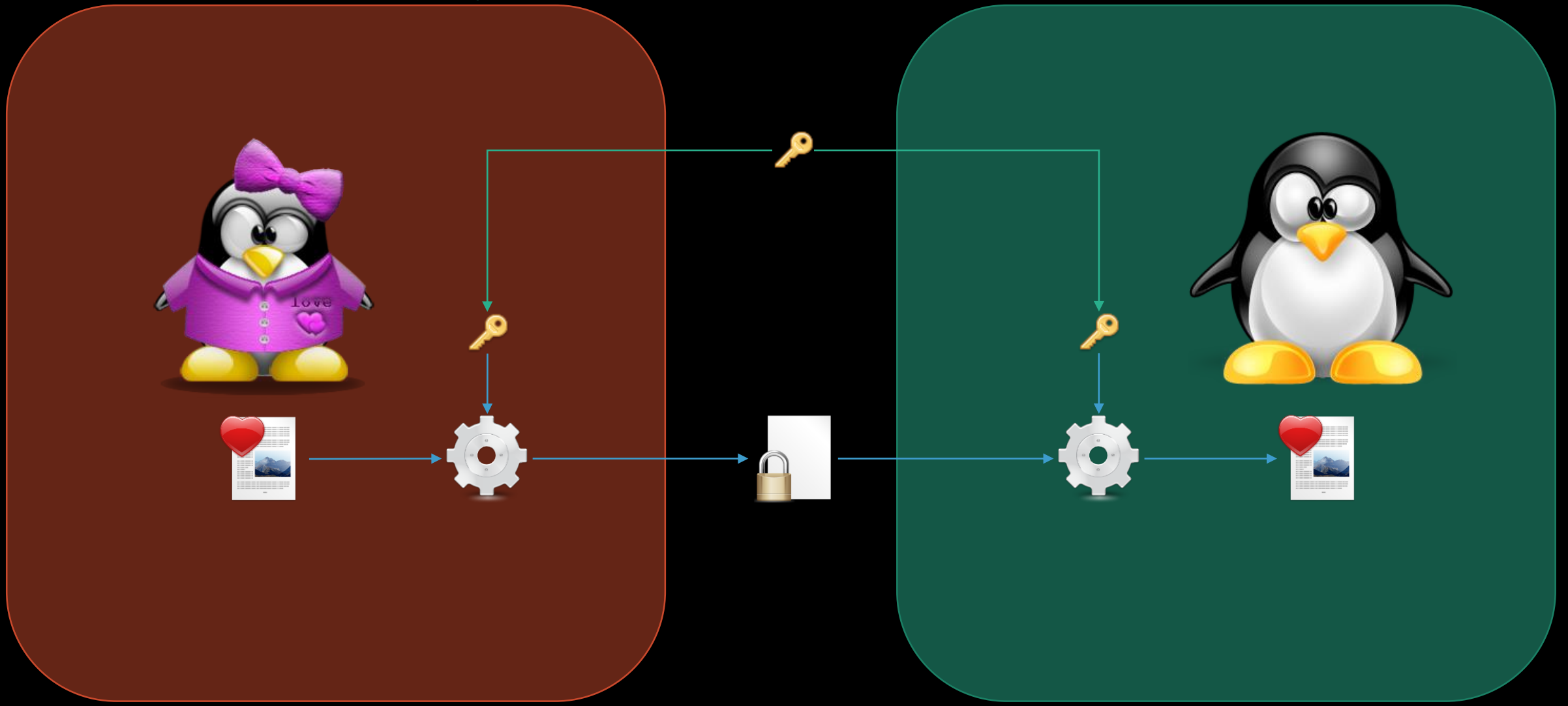
Chiffre avec la clé

déchiffrer avec la même clé



Chiffrer un message

Seul Alice et Bob peuvent le lire



Cryptographie symétrique

Obsolètes

Chiffre de César

4,5 bits

Enigma

67 bits

DES

56 bits

A jour (128 bits)

AES

128 bits

3 DES

112 ou 168 bits

(bientôt obsolète)

Chiffrement par blocs

Problème ?

Algorithmes par blocs

(i.e. 56, 64, 128 bits)

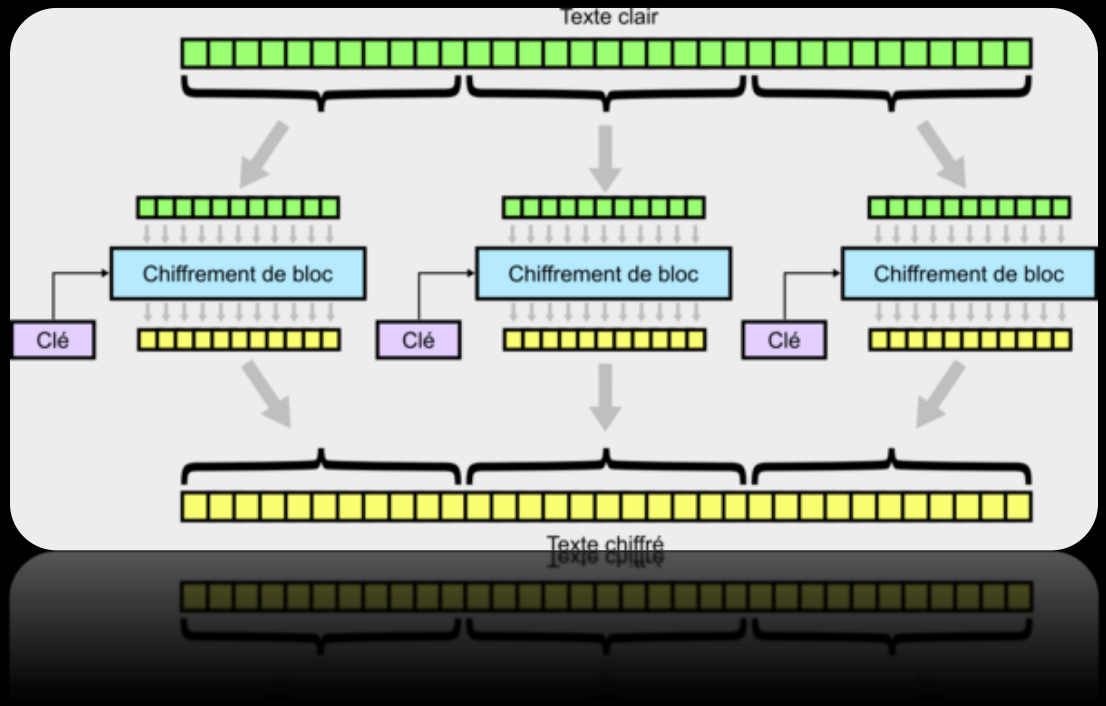
Donnée plus grande

(i.e. Ko, Mo, Go)

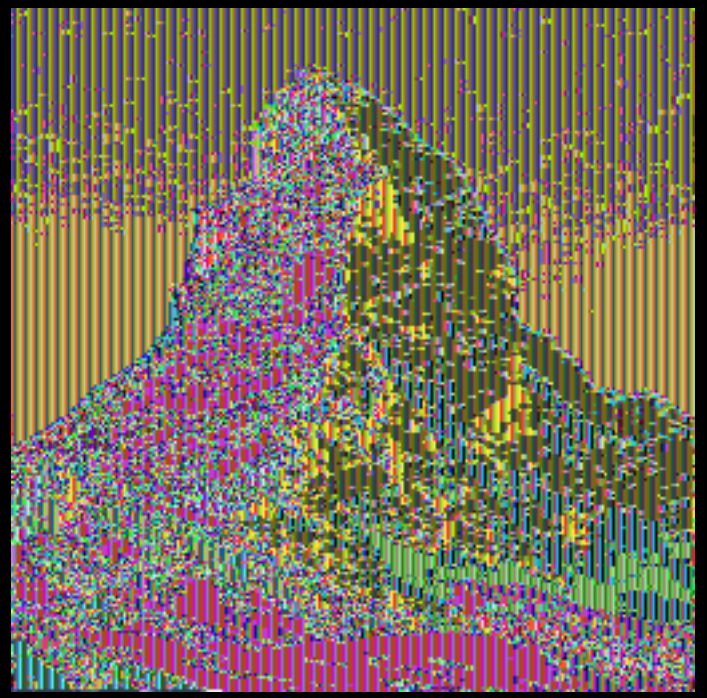
https://commons.wikimedia.org/wiki/File:No_ecb_mode_picture.png

Mode ECB

Blocs individuels



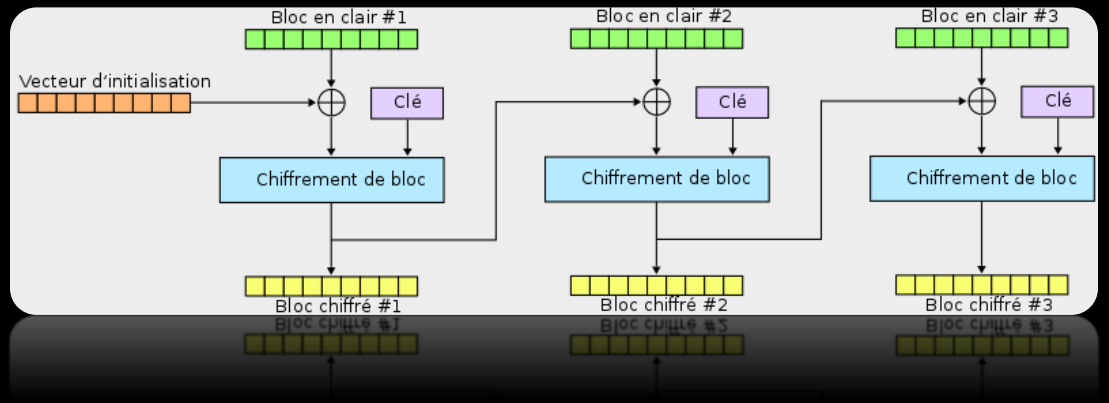
https://commons.wikimedia.org/wiki/File:Schema_ecb.png



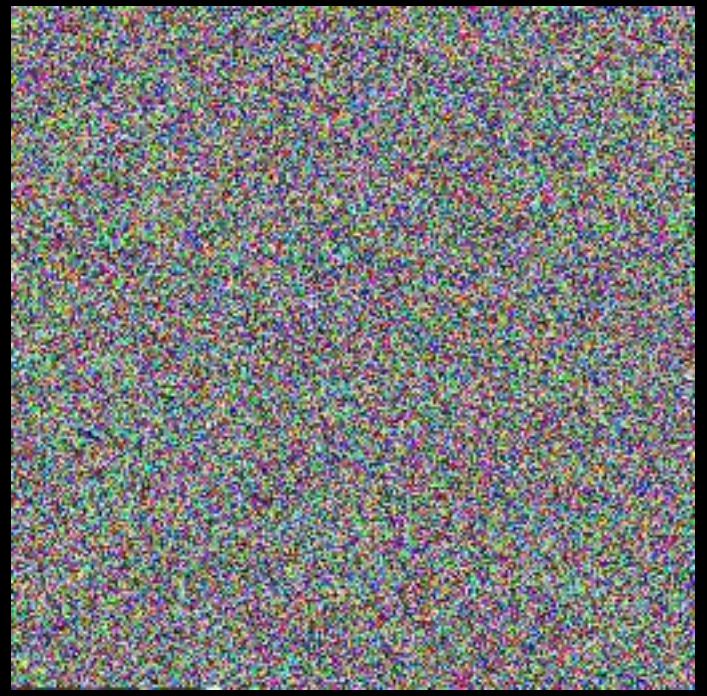
https://commons.wikimedia.org/wiki/File:Ecb_mode_pic.png

Mode CBC

Blocs chiffrés à la chaîne



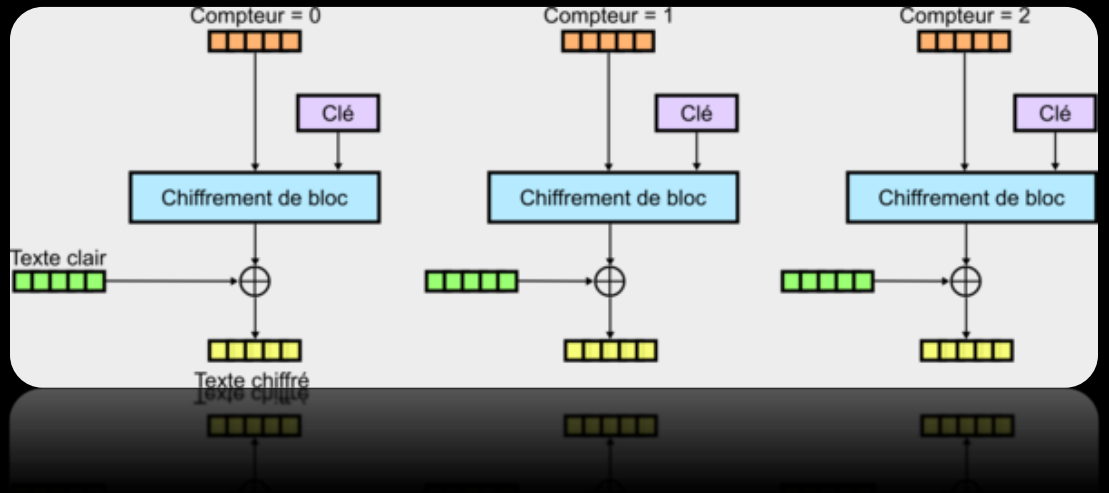
https://commons.wikimedia.org/wiki/File:Schema_CBC.svg



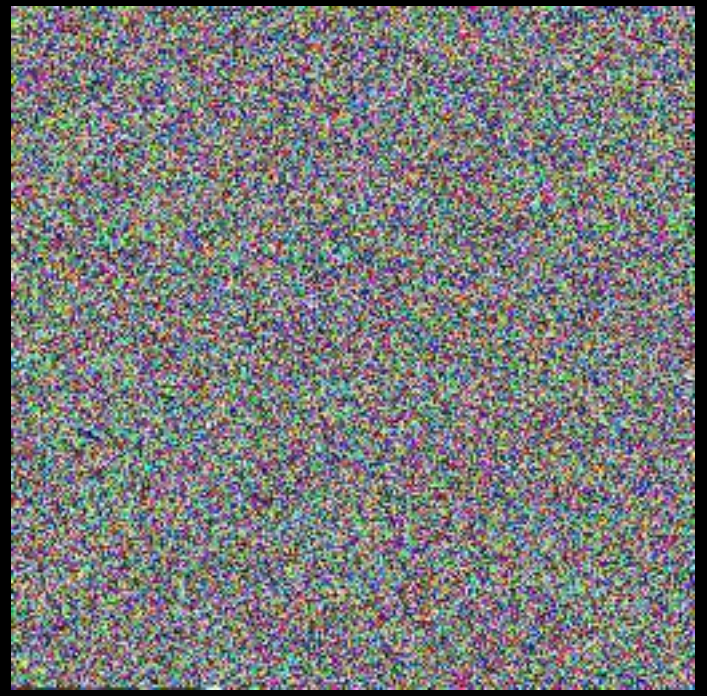
https://commons.wikimedia.org/wiki/File:Cbc_mode_pic.png

Mode CTR

Utilisation d’un compteur / offset



https://commons.wikimedia.org/wiki/File:Schema_ctr.png

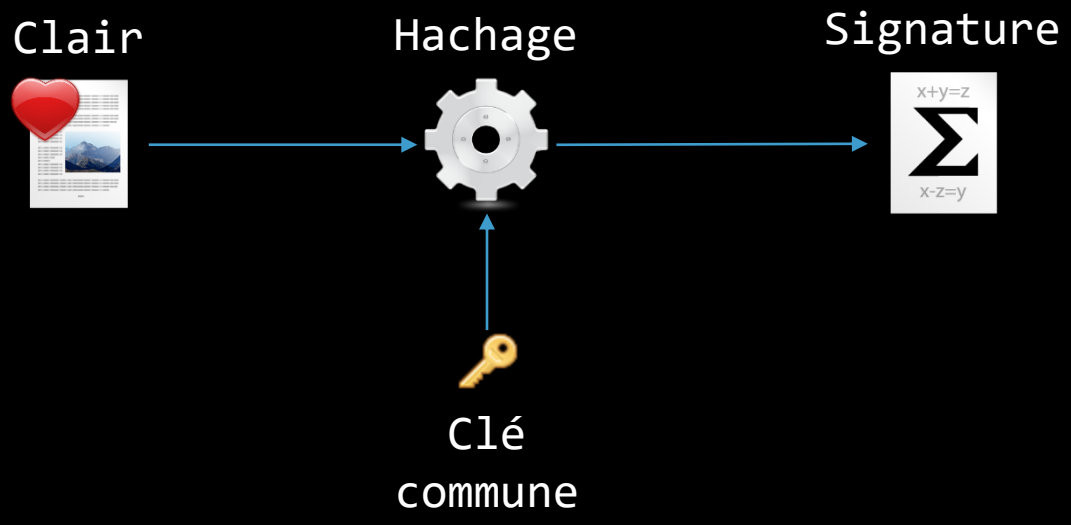


https://commons.wikimedia.org/wiki/File:Cbc_mode_pic.png

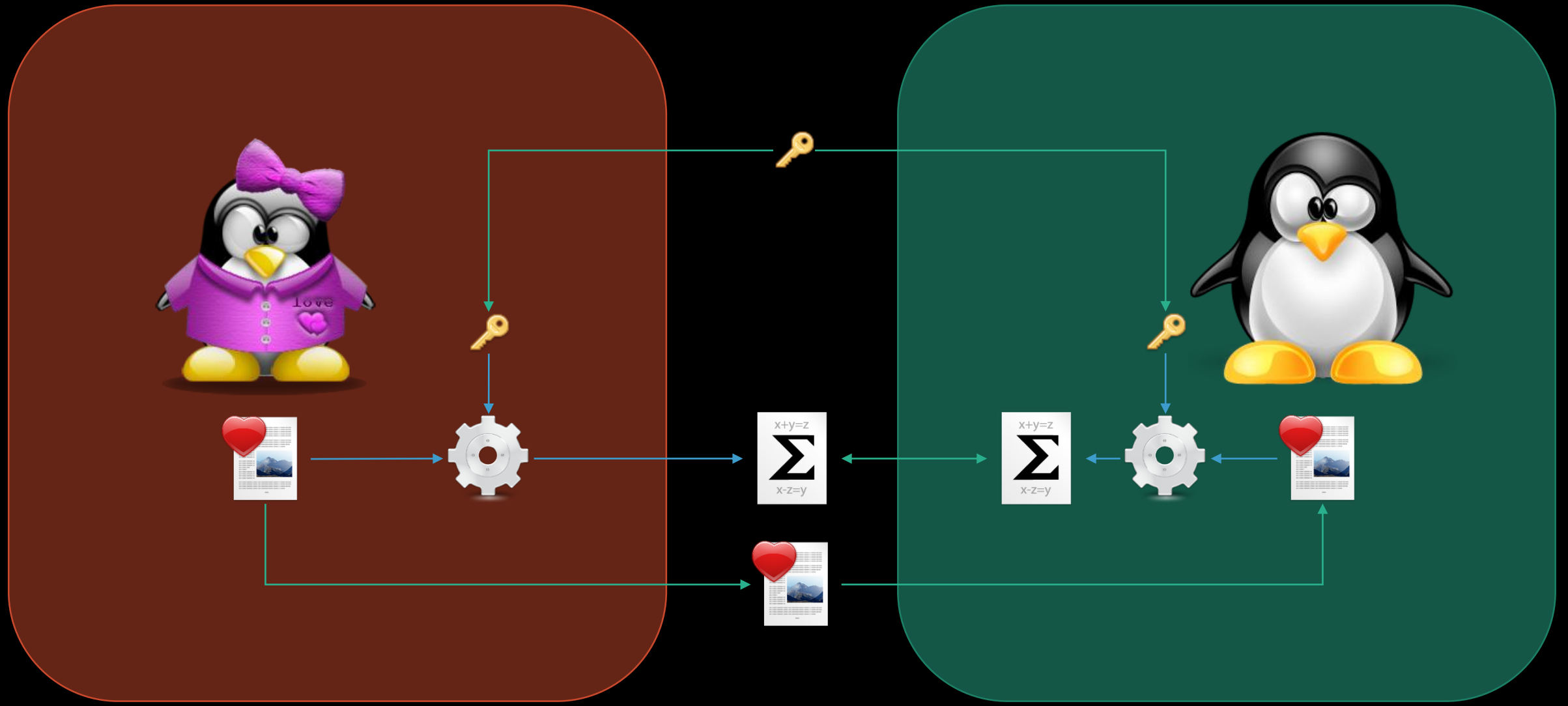
Authenticité symétrique

Authentifier avec la clé

Via des fonctions de hachage



Authentifier un message



Echange de clé

Protocole Diffie-Hellman

Canal de communication non sûr

Eve écoute

Fixer les paramètres

Groupe mathématique, base de l'exposant

Choix d’une couleur

Un nombre aléatoire

g

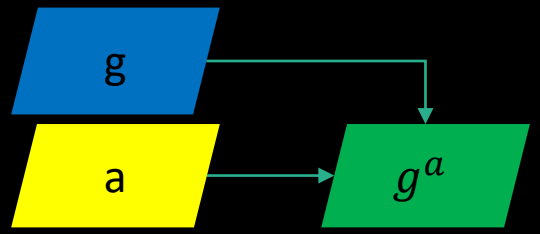
a

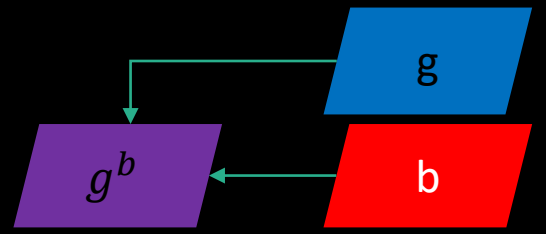
g

b

Mélanger les couleurs

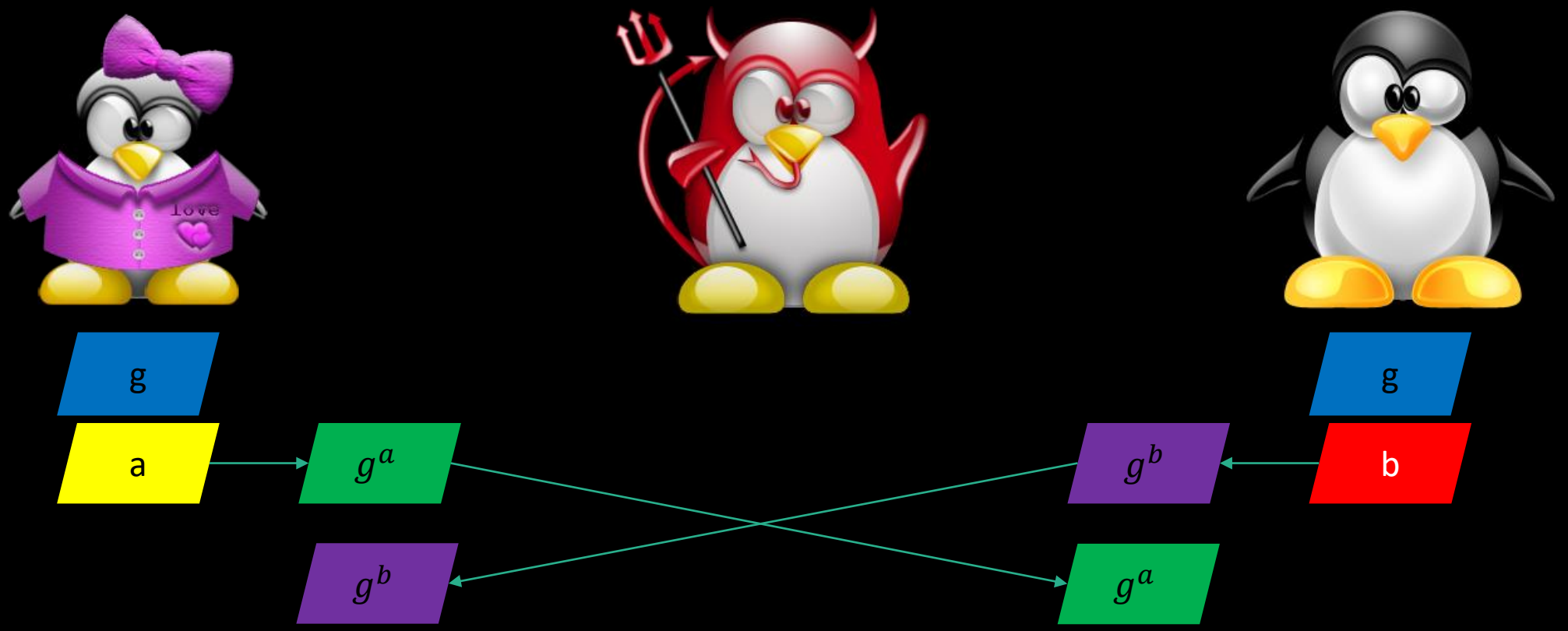
Calculer la puissance





Envoi des couleurs

Les nombres calculés



Mélange des couleurs

Calcul de puissance

g

a

g^{b^a}

g^b

g

b

g^a

g^{ab}

Pourquoi ça converge ?

L’exponentiation est commutative

g^{b^a}

$$g^{b^a} = g^{ba} = g^{ab} = g^{a^b}$$

g^{a^b}

Quand est-ce sûr

Quand le logarithme est difficile

Produit d'entiers modulo N

$(Z/nZ, \times)$

Courbes elliptique