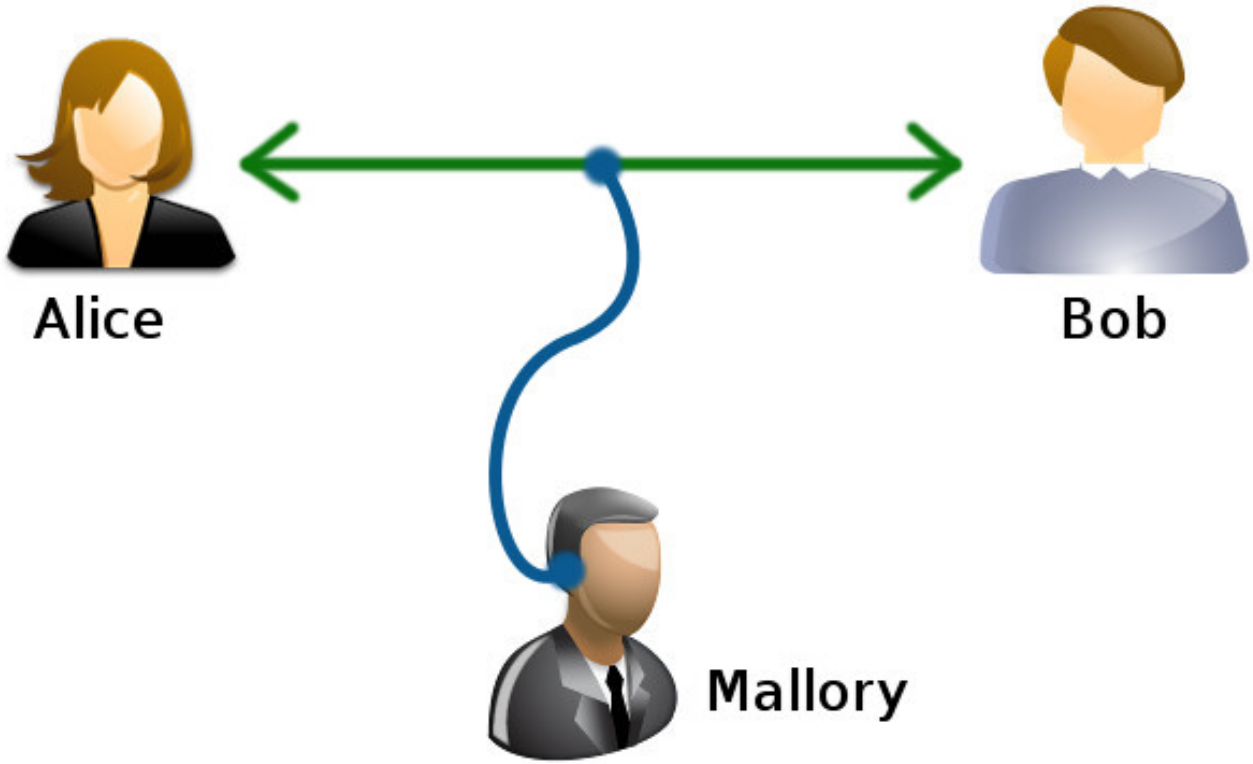
Chiffrement par blocs

HackademINT

23 novembre 2021

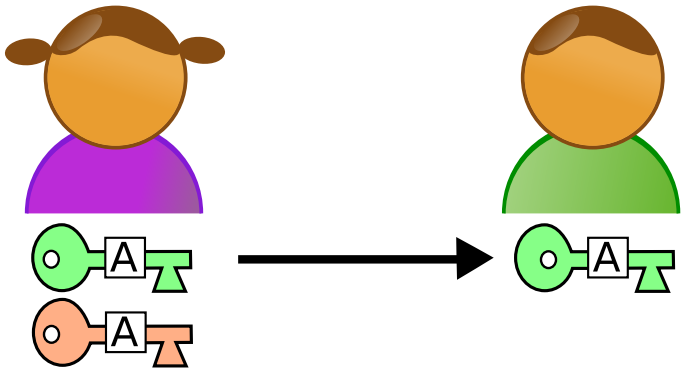
Chiffrement



https://commons.wikimedia.org/wiki/File:Alice-bob-mallory.jpg

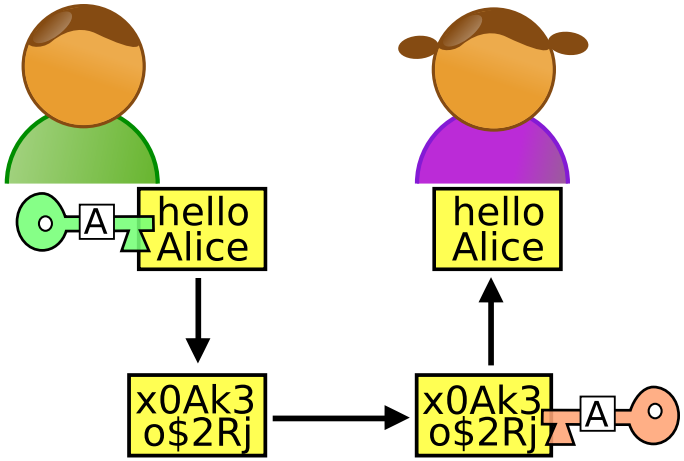
Figure – Représentation d'une attaque

Chiffrement asymétrique



https://commons.wikimedia.org/wiki/File:Asymmetric_cryptography_-_step_1.svg

(a) Création des clés



https://commons.wikimedia.org/wiki/File:Asymmetric_cryptography_-_step_2.svg

(b) Envoi d'un message

Pas de panique !

Principe du RSA

Soit :

- Des entiers p et q premiers distincts. On pose $n = p \times q$
- La fonction indicatrice d'Euler φ : ici, $\varphi(n) = (p-1) \times (q-1)$
- Un entier e tel que :
  1. $1 < e < \varphi(n)$
  2. e et $\varphi(n)$ sont premiers entre eux.

(n, e) est la **clé publique**

Clé privée

Rappel : $\varphi(n) = (p-1) \times (q-1)$

Clé publique : (n, e). Comment obtenir la clé privée ?

On choisit d tel que :

$$d \times e \equiv 1\,[\varphi(n)]$$

C'est à dire qu'on cherche un couple (d, k) tel que :

$$de + k\varphi(n) = 1$$

Clé privée : (n, d)

Chiffrement et déchiffrement

Soit m un message à chiffrer. On pose c ainsi :

$$c = m^e \bmod n$$

c est le *message chiffré*

Opération inverse :

$$m = c^d \bmod n$$