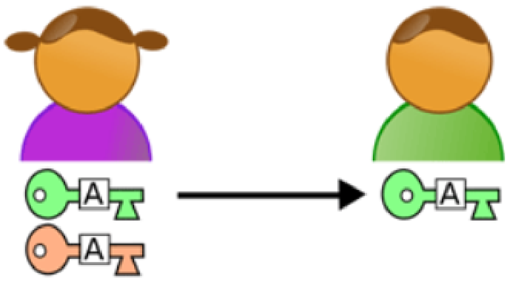
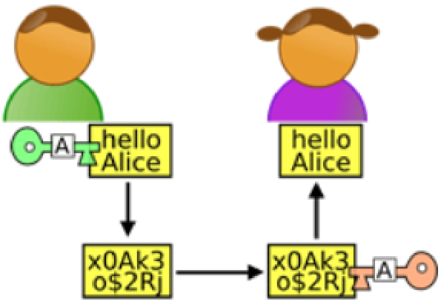
Chiffrement RSA

RSA (initiales des trois inventeurs) est un algorithme de chiffrement, cryptage, asymétrique décrit en 1977 par Ronald **R**ivest, Adi **S**hamir et Leonard **A**dleman.



Principe de la cryptographie asymétrique.
Alice génère deux clés : la clé publique (verte) qu'elle envoie à Bob et la clé privée (rose) qu'elle conserve précieusement sans la divulguer à quiconque.



Bob chiffre son message avec la clé publique d'Alice et lui envoie le texte chiffré. Alice déchiffre le message grâce à sa clé privée.
Source : Wikipédia

Les clés sont des couples de valeurs permettant le calcul de l'information cryptée et de l'information décryptée. La clé publique, par exemple **(33, 3)**, et la clé privée, par exemple **(33, 7)**, sont différentes.

Cryptage à partir de la clé publique (n, e)

Soit un nombre **M**. Son chiffrement est donné par la formule :

$$C = M^e (\mathrm{mod}\, n)$$

On obtient le nombre chiffré **C**. **M** doit être strictement inférieur à **n**.

Chiffrer le nombre **25** à l'aide de la clé publique **(33, 3)**.

....

Décryptage à partir de la clé privée (n, d)

Pour déchiffrer **C** et obtenir **M**, la formule est :

$$M = C^d (\mathrm{mod}\, n)$$

Déchiffrer le nombre chiffré précédent à l'aide de la clé privée **(33, 7)**, puis essayer avec la clé publique.

....

....

https://interstices.info/nombres-premiers-et-cryptologie-lalgorithme-rsa/
https://fr.wikipedia.org/wiki/Cryptographie_asymétrique

Génération des clés

Il faut suivre la procédure ci-dessous. A titre d'exemple, l'appliquer pour des petits nombres.

1. Choisir **p** et **q**, deux nombres premiers distincts.
....

2. Calculer leur produit **n = p.q**, appelé module de chiffrement.
....

3. Calculer la valeur de l'indicatrice d'Euler **φ** en n $\varphi(n)=(p-1)\times(q-1)$.
....

4. Choisir un entier naturel **e** premier avec **φ(n)** et strictement inférieur à **φ(n)**, appelé exposant de chiffrement.
....
....

5. Calculer l'entier naturel **d**, inverse de **e** modulo **φ(n)**, et strictement inférieur à **φ(n)**, appelé exposant de déchiffrement. **d** peut se calculer efficacement par l'algorithme d'Euclide étendu.
....
....

6. Vérifier que la clé publique **(n, e)** et la clé privée **(n, d)** permettent de chiffrer et déchiffrer selon la méthode RSA. Il sera possible de considérer le chiffre **M = 25**.
....
....

Le modulo
C'est le reste **r** de la division euclidienne de deux entiers naturels **a** et **b** : $r=a \bmod b$

On dit de **r** est congrue à **a** modulo **b**, noté : $r \equiv a \pmod b$

L'inverse modulaire
Soit **u** l'inverse de **a** modulo **b** : $u \equiv a^{-1} \pmod b$ est tel que $a.u \equiv 1 \pmod b$

En pratique si on ne travaille qu'avec des entiers naturels, on peut chercher le nombre **u** tel que :

$$a.u=1+v.b \quad \text{avec} \quad v=0,1,2,3,\ldots$$

Nombres premiers
Un nombre premier est un entier naturel qui admet exactement deux diviseurs distincts entiers et positifs. Ces deux diviseurs sont **1** et le nombre considéré. **1** n'est pas un nombre premier.

Nombres premiers entre eux
Deux entiers a et b sont premiers entre eux si leur plus grand commun diviseur est égal à 1, en d'autres termes, s'ils n'ont aucun diviseur autre que 1 et –1 en commun. De manière équivalente, ils sont premiers entre eux s'ils n'ont aucun facteur premier en commun.

Le plus grand commun diviseur
Le **PGCD** de deux nombres entiers non nuls est le plus grand entier qui les divise simultanément.

https://fr.wikipedia.org/wiki/Indicatrice_d'Euler
http://jf.burnol.free.fr/agreg171124euclide_info.pdf