Nombres premiers et cryptographie

Loïc Demeulenaere

22 mars 2016

Cryptographie, késaco ?

- Art de chiffrer ("crypter") des messages ou des données
  $\hookrightarrow$ rendre un message incompréhensible pour les non-destinataires !

Cryptographie, késaco ?

- Art de chiffrer ("crypter") des messages ou des données
  $\hookrightarrow$ rendre un message incompréhensible pour les non-destinataires !
- Applications multiples : **sécurité**, **protection des données**, **sécurisation des transactions bancaires sur Internet**,...

Cryptographie, késaco ?

- Art de chiffrer ("crypter") des messages ou des données
  $\hookrightarrow$ rendre un message incompréhensible pour les non-destinataires !
- Applications multiples : **sécurité**, **protection des données**, **sécurisation des transactions bancaires sur Internet**,...
- Équilibre entre sécurité ($\not\Delta$ordinateurs) et facilité de décryptage pour les destinataires

Nombres premiers : rappels !

Rappel...

Nombre premier : nombre entier positif possédant **exactement 2 diviseurs** (en particulier 1 et lui-même)

Nombres premiers : rappels !

Rappel...

Nombre premier : nombre entier positif possédant **exactement 2 diviseurs** (en particulier 1 et lui-même)

Exemples : 2, 3, 5, 7

Nombres premiers : rappels !

Rappel...

Nombre premier : nombre entier positif possédant **exactement 2 diviseurs** (en particulier 1 et lui-même)

Exemples : 2, 3, 5, 7, ... , 101, ..., 7919, ...

Théorème fondamental de l'Arithmétique

Propriété fondamentale

Tout nombre entier > 1 s'écrit comme un **produit de nombres premiers**

Théorème fondamental de l'Arithmétique

Propriété fondamentale

Tout nombre entier > 1 s'écrit comme un **produit de nombres premiers**

Exemples

- $4 = 2 \times 2$, $42 = 2 \times 3 \times 7$, ...

Théorème fondamental de l'Arithmétique

Propriété fondamentale

Tout nombre entier > 1 s'écrit comme un **produit de nombres premiers**

Exemples

- $4 = 2 \times 2$, $42 = 2 \times 3 \times 7$, ...
- $36\,694\,632\,833 = ?$

Théorème fondamental de l'Arithmétique

Propriété fondamentale

Tout nombre entier > 1 s'écrit comme un **produit de nombres premiers**

Exemples

- $4 = 2 \times 2$, $42 = 2 \times 3 \times 7$, ...
- $36\,694\,632\,833 = 104\,729 \times 224\,737$

Constat

Très difficile de décomposer un nombre en nombres premiers : **beaucoup de calculs** !

Exemple : pour un ordinateur, décomposer un nombre de **300 chiffres peut prendre des milliards de... millénaires** !

RSA

Alice veut envoyer des messages cryptés à Bob !

RSA

Alice veut envoyer des messages cryptés à Bob !

- Bob : choix d'un grand nombre (**300 à 600 chiffres**)
  = produit de **2 nombres premiers (150 à 300 chiffres)**

RSA

Alice veut envoyer des messages cryptés à Bob !

- Bob : choix d'un grand nombre (**300 à 600 chiffres**)
  = produit de **2 nombres premiers (150 à 300 chiffres)**
- RSA $\rightarrow$ à partir des nombres premiers, calcul de l'exposant de chiffrement et de l'exposant de déchiffrement

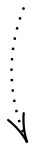
RSA

Alice veut envoyer des messages cryptés à Bob !

- Bob : choix d'un grand nombre (**300 à 600 chiffres**)
  = produit de **2 nombres premiers (150 à 300 chiffres)**
- RSA $\rightarrow$ à partir des nombres premiers, calcul de l'exposant de chiffrement et de l'exposant de déchiffrement
- *Public* : grand nombre et exposant de chiffrement
- *Secret* **[Sécurité]** : nombres premiers et exposant de déchiffrement

RSA

1. Bob publie le grand nombre et l'exposant de chiffrement

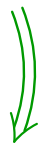


2. Alice crypte son *message* grâce aux grand nombre et exposant de chiffrement

3. Alice envoie le message crypté

Danger ! Pirate ?

4. Bob reçoit le message crypté



5. Bob décrypte le message grâce aux grand nombre et exposant de déchiffrement

Merci pour votre attention ! $\leftrightsquigarrow$ Phufl srxu yrwuh dwwhqwlrq !