Algorithmique et cryptographie

Emmanuel Hallouin

Institut de Mathématiques de Toulouse

Toulouse, 14 Février 2018

Communications numériques

Communications numériques

Voici une liste de qualités que l'on souhaite retrouver lors d'échange d'informations ou données numériques

Communications numériques

Voici une liste de qualités que l'on souhaite retrouver lors d'échange d'informations ou données numériques

- leur confidentialité : assurance que ces informations n'ont pas été interceptées (lettre envoyé par la poste, secret dévoilé au coin de l'oreille)

Communications numériques

Voici une liste de qualités que l'on souhaite retrouver lors d'échange d'informations ou données numériques

- leur confidentialité : assurance que ces informations n'ont pas été interceptées (lettre envoyé par la poste, secret dévoilé au coin de l'oreille)
- leur intégrité : assurance que les informations n'ont pas été altérées (paquetage tout neuf, copie conforme)

Communications numériques

Voici une liste de qualités que l'on souhaite retrouver lors d'échange d'informations ou données numériques

- leur confidentialité : assurance que ces informations n'ont pas été interceptées (lettre envoyé par la poste, secret dévoilé au coin de l'oreille)
- leur intégrité : assurance que les informations n'ont pas été altérées (paquetage tout neuf, copie conforme)
- leur authentification : garanties sur l'origine des informations (simple contact visuel, présentation de papiers d'identité)

Communications numériques

Voici une liste de qualités que l'on souhaite retrouver lors d'échange d'informations ou données numériques

- leur confidentialité : assurance que ces informations n'ont pas été interceptées (lettre envoyé par la poste, secret dévoilé au coin de l'oreille)
- leur intégrité : assurance que les informations n'ont pas été altérées (paquetage tout neuf, copie conforme)
- leur authentification : garanties sur l'origine des informations (simple contact visuel, présentation de papiers d'identité)
- leur non répudiation : l'expéditeur ne peut pas nier ultérieurement avoir envoyé ces informations (signature apposée au bas du chèque)

Communications numériques

Voici une liste de qualités que l'on souhaite retrouver lors d'échange d'informations ou données numériques

- leur confidentialité : assurance que ces informations n'ont pas été interceptées (lettre envoyé par la poste, secret dévoilé au coin de l'oreille)
- leur intégrité : assurance que les informations n'ont pas été altérées (paquetage tout neuf, copie conforme)
- leur authentification : garanties sur l'origine des informations (simple contact visuel, présentation de papiers d'identité)
- leur non répudiation : l'expéditeur ne peut pas nier ultérieurement avoir envoyé ces informations (signature apposée au bas du chèque)

Transit via un canal non sécurisé (ex. le `web`)

Crypto-système

Formalisation d'un crypto-système

Formalisation d'un crypto-système

C'est la donnée

Crypto-système

Formalisation d'un crypto-système

C'est la donnée

- d'un ensemble de messages clairs $\mathcal{P}$,

Crypto-système

Formalisation d'un crypto-système

C'est la donnée

- d'un ensemble de messages clairs $\mathcal{P}$,
- d'un ensemble de messages chiffrés $\mathcal{C}$,

Crypto-système

Formalisation d'un crypto-système

C'est la donnée

- d'un ensemble de messages clairs $\mathcal{P}$,
- d'un ensemble de messages chiffrés $\mathcal{C}$,
- d'un ensemble de clés $\mathcal{K}$,

Crypto-système

Formalisation d'un crypto-système

C'est la donnée

- d'un ensemble de messages clairs $\mathcal{P}$,
- d'un ensemble de messages chiffrés $\mathcal{C}$,
- d'un ensemble de clés $\mathcal{K}$,

tels que à toute clé $\kappa \in \mathcal{K}$, il correspond une application C_κ de chiffrement et une autre D_κ de déchiffrement, réciproques l'une de l'autre :

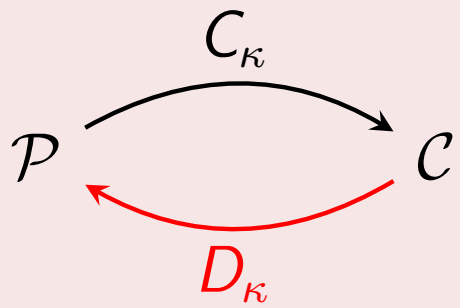
Crypto-système

Formalisation d'un crypto-système

C'est la donnée

- d'un ensemble de messages clairs $\mathcal{P}$,
- d'un ensemble de messages chiffrés $\mathcal{C}$,
- d'un ensemble de clés $\mathcal{K}$,

tels que à toute clé $\kappa \in \mathcal{K}$, il correspond une application C_κ de chiffrement et une autre D_κ de déchiffrement, réciproques l'une de l'autre :



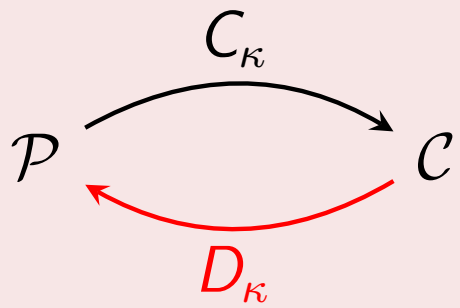
Crypto-système

Formalisation d'un crypto-système

C'est la donnée

- d'un ensemble de messages clairs $\mathcal{P}$,
- d'un ensemble de messages chiffrés $\mathcal{C}$,
- d'un ensemble de clés $\mathcal{K}$,

tels que à toute clé $\kappa \in \mathcal{K}$, il correspond une application C_κ de chiffrement et une autre D_κ de déchiffrement, réciproques l'une de l'autre :



$$\forall m \in \mathcal{P},$$
$$D_\kappa(C_\kappa(m)) = m$$

Deux types de cryptographie

Deux types de cryptographie

À clé privée

Les deux applications de chiffrement et de déchiffrement sont secrètes.

Deux types de cryptographie

À clé privée

Les deux applications de chiffrement et de déchiffrement sont secrètes.

À clé publique

L'application de chiffrement est publique tandis que celle de déchiffrement est secrète.

Deux types de cryptographie

À clé privée

Les deux applications de chiffrement et de déchiffrement sont secrètes.

- **Avantages**
  - Simplicité
  - Rapidité/Efficacité
- **Désavantages**
  - Nécessite un pré-accord
  - Vulnérable aux attaques

À clé publique

L'application de chiffrement est publique tandis que celle de déchiffrement est secrète.

Deux types de cryptographie

À clé privée

Les deux applications de chiffrement et de déchiffrement sont secrètes.

- **Avantages**
  - Simplicité
  - Rapidité/Efficacité
- **Désavantages**
  - Nécessite un pré-accord
  - Vulnérable aux attaques

À clé publique

L'application de chiffrement est publique tandis que celle de déchiffrement est secrète.

- **Avantages**
  - Souplesse d'utilisation
  - Robustesse
- **Désavantages**
  - Difficulté de mise en oeuvre
  - Lenteur/Énergivore

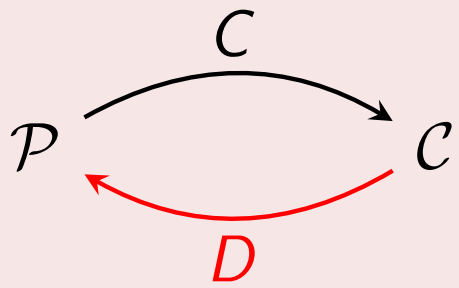
La pierre d'achoppement

Fonction asymétrique munie d'une trappe

La pierre d'achoppement

Fonction asymétrique munie d'une trappe

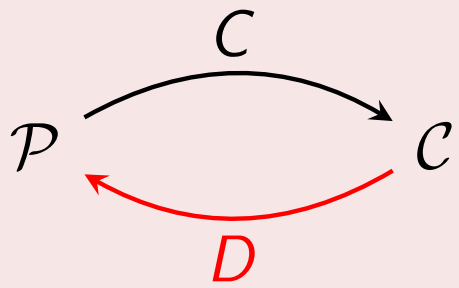
Une fonction asymétrique est une bijection présentant une dissymétrie en terme d'efficacité de calculs :



La pierre d'achoppement

Fonction asymétrique munie d'une trappe

Une fonction asymétrique est une bijection présentant une dissymétrie en terme d'efficacité de calculs :

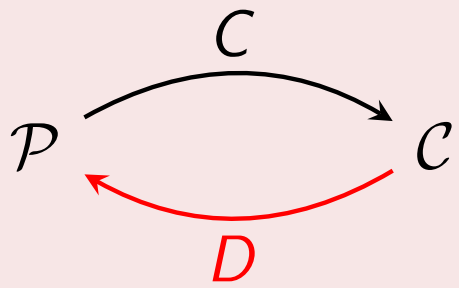


- l'application C est facile à calculer

La pierre d'achoppement

Fonction asymétrique munie d'une trappe

Une fonction asymétrique est une bijection présentant une dissymétrie en terme d'efficacité de calculs :

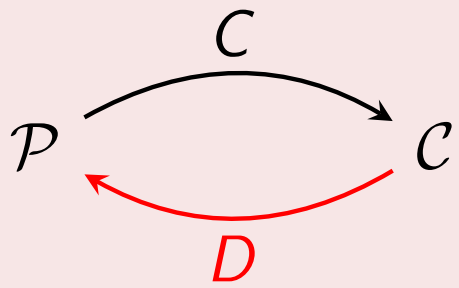


- l'application C est facile à calculer
- l'application réciproque D est difficile à calculer

La pierre d'achoppement

Fonction asymétrique munie d'une trappe

Une fonction asymétrique est une bijection présentant une dissymétrie en terme d'efficacité de calculs :



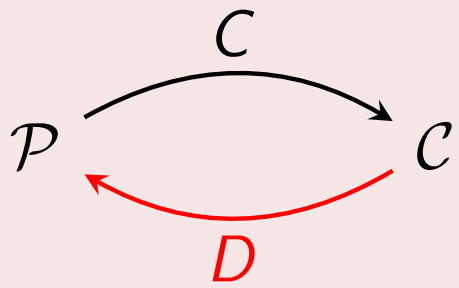
- l'application C est facile à calculer
- l'application réciproque D est difficile à calculer

Cette fonction doit être munie d'une trappe, c'est-à-dire :

La pierre d'achoppement

Fonction asymétrique munie d'une trappe

Une fonction asymétrique est une bijection présentant une dissymétrie en terme d'efficacité de calculs :



- l'application C est facile à calculer
- l'application réciproque D est difficile à calculer

Cette fonction doit être munie d'une trappe, c'est-à-dire :

- une information supplémentaire rendant le calcul de la réciproque D facile.

Confidentialité

Confidentialité

Si Alice veut rentrer en contact avec Bob via un réseau non sécurisé

Confidentialité

Si Alice veut rentrer en contact avec Bob via un réseau non sécurisé

- Alice récupère la clé publique de Bob (sur son site web ou dans un annuaire)

Confidentialité

Si Alice veut rentrer en contact avec Bob via un réseau non sécurisé

- Alice récupère la clé publique de Bob (sur son site web ou dans un annuaire)
- Alice chiffre les données qu'elle veut envoyer à Bob avec la clé publique de Bob

Confidentialité

Si Alice veut rentrer en contact avec Bob via un réseau non sécurisé

- Alice récupère la clé publique de Bob (sur son site web ou dans un annuaire)
- Alice chiffre les données qu'elle veut envoyer à Bob avec la clé publique de Bob
- Ces données chiffrées sont envoyées par Alice à Bob via le réseau

Confidentialité

Si Alice veut rentrer en contact avec Bob via un réseau non sécurisé

- Alice récupère la clé publique de Bob (sur son site web ou dans un annuaire)
- Alice chiffre les données qu'elle veut envoyer à Bob avec la clé publique de Bob
- Ces données chiffrées sont envoyées par Alice à Bob via le réseau
- Après réception des données, Bob peut les déchiffrer avec sa clé privée

Authentification Signature

Authentification Signature

Alice veut envoyer des données à Bob de telle sorte que ce dernier puisse authentifier leur source.

Authentification Signature

Alice veut envoyer des données à Bob de telle sorte que ce dernier puisse authentifier leur source.

- Alice chiffre les données qu'elle souhaite envoyer à Bob avec sa propre clé privée ; ce chiffrement fait office de signature

Authentification Signature

Alice veut envoyer des données à Bob de telle sorte que ce dernier puisse authentifier leur source.

- Alice chiffre les données qu'elle souhaite envoyer à Bob avec sa propre clé privée ; ce chiffrement fait office de signature
- Alice envoie les données accompagnées du chiffrement/signature à Bob via le réseau

Authentification Signature

Alice veut envoyer des données à Bob de telle sorte que ce dernier puisse authentifier leur source.

- Alice chiffre les données qu'elle souhaite envoyer à Bob avec sa propre clé privée ; ce chiffrement fait office de signature
- Alice envoie les données accompagnées du chiffrement/signature à Bob via le réseau
- Après réception des données, Bob peut déchiffrer la partie signature du message reçu avec la clé publique d'Alice et ainsi vérifier qu'elle coïncide avec la partie en clair du message reçu.

Et l'arithmétique devint «utile» !

Et l'arithmétique devint «utile» !

Les fonctions asymétriques munies d'une trappe ne courent pas les rues... et l'arithmétique s'avère le meilleur pourvoyeur de telles fonctions :

Et l'arithmétique devint «utile» !

Les fonctions asymétriques munies d'une trappe ne courent pas les rues... et l'arithmétique s'avère le meilleur pourvoyeur de telles fonctions :

- Protocole ElGamal (puissance, logarithme discret) dans un (gros) corps fini

Et l'arithmétique devint «utile» !

Les fonctions asymétriques munies d'une trappe ne courent pas les rues... et l'arithmétique s'avère le meilleur pourvoyeur de telles fonctions :

- Protocole ElGamal (puissance, logarithme discret) dans un (gros) corps fini
- Protocole RSA (Rivest, Shamir, Adlemann) (produit, factorisation) de grands entiers

Et l'arithmétique devint «utile» !

Les fonctions asymétriques munies d'une trappe ne courent pas les rues... et l'arithmétique s'avère le meilleur pourvoyeur de telles fonctions :

- Protocole ElGamal (puissance, logarithme discret) dans un (gros) corps fini
- Protocole RSA (Rivest, Shamir, Adlemann) (produit, factorisation) de grands entiers
- Protocole à base de courbes elliptiques, (multiplication, division) d'un point de la courbe par un entier

L'ensemble $\mathbb{Z}/n\mathbb{Z}$, des classes modulo n

L'ensemble $\mathbb{Z}/n\mathbb{Z}$, des classes modulo n

A tout $n \geq 2$, on associe la répartition suivante en classes

L'ensemble $\mathbb{Z}/n\mathbb{Z}$, des classes modulo n

A tout $n \geq 2$, on associe la répartition suivante en classes

$$\overline{0} = \{nk,\ k \in \mathbb{Z}\}$$

L'ensemble $\mathbb{Z}/n\mathbb{Z}$, des classes modulo n

A tout $n \geq 2$, on associe la répartition suivante en classes

$$\overline{0} = \{nk,\ k \in \mathbb{Z}\}$$
$$\overline{1} = \{1 + nk,\ k \in \mathbb{Z}\}$$

L'ensemble $\mathbb{Z}/n\mathbb{Z}$, des classes modulo n

A tout $n \geq 2$, on associe la répartition suivante en classes

$$\overline{0} = \{nk,\ k \in \mathbb{Z}\}$$
$$\overline{1} = \{1 + nk,\ k \in \mathbb{Z}\}$$
$$\vdots$$
$$\overline{n-1} = \{n - 1 + nk,\ k \in \mathbb{Z}\}$$

L'ensemble $\mathbb{Z}/n\mathbb{Z}$, des classes modulo n

A tout $n \geq 2$, on associe la répartition suivante en classes

$$\begin{aligned}
\overline{0} &= \{nk,\ k \in \mathbb{Z}\} \\
\overline{1} &= \{1 + nk,\ k \in \mathbb{Z}\} \\
&\vdots \\
\overline{n-1} &= \{n - 1 + nk,\ k \in \mathbb{Z}\}
\end{aligned}$$

On décrète l'égalité entre tous les entiers d'une même classe, si bien que pour $x, y \in \mathbb{Z}$, on a

$$\overline{x} = \overline{y} \quad \Leftrightarrow \quad x \equiv y \pmod{n} \quad \Leftrightarrow \quad n \mid (x - y)$$

L'ensemble $\mathbb{Z}/n\mathbb{Z}$, des classes modulo n

A tout $n \geq 2$, on associe la répartition suivante en classes

$$\begin{aligned}
\overline{0} &= \{nk,\ k \in \mathbb{Z}\} \\
\overline{1} &= \{1 + nk,\ k \in \mathbb{Z}\} \\
&\vdots \\
\overline{n-1} &= \{n - 1 + nk,\ k \in \mathbb{Z}\}
\end{aligned}$$

On décrète l'égalité entre tous les entiers d'une même classe, si bien que pour $x, y \in \mathbb{Z}$, on a

$$\overline{x} = \overline{y} \quad \Leftrightarrow \quad x \equiv y \pmod{n} \quad \Leftrightarrow \quad n \mid (x - y)$$

et

$$\overline{x} = \overline{x \bmod n}$$

où $x \bmod n$ est le reste de la division euclidienne de x par n.

Le seigneur des «anneaux» : $(\mathbb{Z}/n\mathbb{Z}, +, \times)$

Le seigneur des «anneaux» : $(\mathbb{Z}/n\mathbb{Z}, +, \times)$

On vérifie aisément que les lois d'addition et de multiplication sur les entiers passent bien aux classes. Il est légtime de définir la somme et le produit de deux classes via :

Le seigneur des «anneaux» : $(\mathbb{Z}/n\mathbb{Z}, +, \times)$

On vérifie aisément que les lois d'addition et de multiplication sur les entiers passent bien aux classes. Il est légtime de définir la somme et le produit de deux classes via :

$$\overline{x} + \overline{y} = \overline{x + y} \qquad \overline{x} \times \overline{y} = \overline{x \times y}$$

Le seigneur des «anneaux» : $(\mathbb{Z}/n\mathbb{Z}, +, \times)$

On vérifie aisément que les lois d'addition et de multiplication sur les entiers passent bien aux classes. Il est légtime de définir la somme et le produit de deux classes via :

$$\overline{x} + \overline{y} = \overline{x + y} \qquad \overline{x} \times \overline{y} = \overline{x \times y}$$

Muni de ces deux lois, l'ensemble des classes $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ devient un anneau.

Le seigneur des «anneaux» : $(\mathbb{Z}/n\mathbb{Z}, +, \times)$

On vérifie aisément que les lois d'addition et de multiplication sur les entiers passent bien aux classes. Il est légtime de définir la somme et le produit de deux classes via :

$$\overline{x} + \overline{y} = \overline{x + y} \qquad \overline{x} \times \overline{y} = \overline{x \times y}$$

Muni de ces deux lois, l'ensemble des classes $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ devient un anneau.

Cas particuliers :

- p premier $\Rightarrow \mathbb{Z}/p\mathbb{Z}$ est un corps fini
- RSA $\Rightarrow \mathbb{Z}/pq\mathbb{Z}$, $p \neq q$ premiers

À table(s) !

À table(s) !

$\mathbb{Z}/5\mathbb{Z}$

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

À table(s) !

$\mathbb{Z}/5\mathbb{Z}$

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

$\mathbb{Z}/6\mathbb{Z}$

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Groupe des inversibles modulo n : $(\mathbb{Z}/n\mathbb{Z}^*, \times)$

Groupe des inversibles modulo n : $(\mathbb{Z}/n\mathbb{Z}^*, \times)$

Inversible modulo n

Une classe $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$ est dite **inversible** s'il existe $\overline{y}$ telle que $\overline{x} \times \overline{y} = \overline{1}$. On dit aussi que l'entier $x \in \mathbb{Z}$ est **inversible** modulo n.

Groupe des inversibles modulo n : $(\mathbb{Z}/n\mathbb{Z}^*, \times)$

Inversible modulo n

Une classe $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$ est dite **inversible** s'il existe $\overline{y}$ telle que $\overline{x} \times \overline{y} = \overline{1}$. On dit aussi que l'entier $x \in \mathbb{Z}$ est **inversible** modulo n.

Caractérisation de l'inversibilité modulo n

On a l'équivalence :

$$\overline{x} \in \mathbb{Z}/n\mathbb{Z} \text{ est inversible} \iff \text{pgcd}(x, n) = 1$$

Groupe des inversibles modulo n : $(\mathbb{Z}/n\mathbb{Z}^*, \times)$

Inversible modulo n

Une classe $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$ est dite **inversible** s'il existe $\overline{y}$ telle que $\overline{x} \times \overline{y} = \overline{1}$. On dit aussi que l'entier $x \in \mathbb{Z}$ est **inversible** modulo n.

Caractérisation de l'inversibilité modulo n

On a l'équivalence :

$$\overline{x} \in \mathbb{Z}/n\mathbb{Z} \text{ est inversible} \iff \text{pgcd}(x, n) = 1$$

Exemple : $n = 21$,

$$\mathbb{Z}/21\mathbb{Z}^* = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$$

Une autre caractérisation du pgcd

Une autre caractérisation du pgcd

Thérème de Bezout

Soit $a, b \in \mathbb{Z}$ alors il existe $u, v \in \mathbb{Z}$ tels que :

$$au + bv = \text{pgcd}(a, b)$$

Une autre caractérisation du pgcd

Thérème de Bezout

Soit $a, b \in \mathbb{Z}$ alors il existe $u, v \in \mathbb{Z}$ tels que :

$$au + bv = \text{pgcd}(a, b)$$

L'entier $\text{pgcd}(a, b)$ est l'unique entier (au signe près) qui

- est un diviseur commun de a et b,
- et qui est de la forme $au + bv$ avec $u, v \in \mathbb{Z}$.

Une autre caractérisation du pgcd

Thérème de Bezout

Soit $a, b \in \mathbb{Z}$ alors il existe $u, v \in \mathbb{Z}$ tels que :

$$au + bv = \text{pgcd}(a, b)$$

L'entier $\text{pgcd}(a, b)$ est l'unique entier (au signe près) qui

- est un diviseur commun de a et b,
- et qui est de la forme $au + bv$ avec $u, v \in \mathbb{Z}$.

Lien avec $\mathbb{Z}/n\mathbb{Z}^*$. —

Une autre caractérisation du pgcd

Thérème de Bezout

Soit $a, b \in \mathbb{Z}$ alors il existe $u, v \in \mathbb{Z}$ tels que :

$$au + bv = \text{pgcd}(a, b)$$

L'entier $\text{pgcd}(a, b)$ est l'unique entier (au signe près) qui

- est un diviseur commun de a et b,
- et qui est de la forme $au + bv$ avec $u, v \in \mathbb{Z}$.

Lien avec $\mathbb{Z}/n\mathbb{Z}^*$. — Soit $x \in \mathbb{Z}$:

Une autre caractérisation du pgcd

Thérème de Bezout

Soit $a, b \in \mathbb{Z}$ alors il existe $u, v \in \mathbb{Z}$ tels que :

$$au + bv = \text{pgcd}(a, b)$$

L'entier $\text{pgcd}(a, b)$ est l'unique entier (au signe près) qui

- est un diviseur commun de a et b,
- et qui est de la forme $au + bv$ avec $u, v \in \mathbb{Z}$.

Lien avec $\mathbb{Z}/n\mathbb{Z}^*$. — Soit $x \in \mathbb{Z}$:

$$\text{pgcd}(n, x) = 1$$

Une autre caractérisation du pgcd

Thérème de Bezout

Soit $a, b \in \mathbb{Z}$ alors il existe $u, v \in \mathbb{Z}$ tels que :

$$au + bv = \text{pgcd}(a, b)$$

L'entier $\text{pgcd}(a, b)$ est l'unique entier (au signe près) qui

- est un diviseur commun de a et b,
- et qui est de la forme $au + bv$ avec $u, v \in \mathbb{Z}$.

Lien avec $\mathbb{Z}/n\mathbb{Z}^*$. — Soit $x \in \mathbb{Z}$:

$$\text{pgcd}(n, x) = 1 \quad \Longrightarrow \quad \exists u, v \in \mathbb{Z},\ nu + xv = 1$$

Une autre caractérisation du pgcd

Thérème de Bezout

Soit $a, b \in \mathbb{Z}$ alors il existe $u, v \in \mathbb{Z}$ tels que :

$$au + bv = \text{pgcd}(a, b)$$

L'entier $\text{pgcd}(a, b)$ est l'unique entier (au signe près) qui

- est un diviseur commun de a et b,
- et qui est de la forme $au + bv$ avec $u, v \in \mathbb{Z}$.

Lien avec $\mathbb{Z}/n\mathbb{Z}^*$. — Soit $x \in \mathbb{Z}$:

$$\text{pgcd}(n, x) = 1 \quad \Longrightarrow \quad \exists u, v \in \mathbb{Z},\ nu + xv = 1$$

$$\overset{\text{mod } n}{\Longrightarrow} \quad \overline{n} \times \overline{u} + \overline{x} \times \overline{v} = \overline{1}$$

Une autre caractérisation du pgcd

Thérème de Bezout

Soit $a, b \in \mathbb{Z}$ alors il existe $u, v \in \mathbb{Z}$ tels que :

$$au + bv = \text{pgcd}(a, b)$$

L'entier $\text{pgcd}(a, b)$ est l'unique entier (au signe près) qui

- est un diviseur commun de a et b,
- et qui est de la forme $au + bv$ avec $u, v \in \mathbb{Z}$.

Lien avec $\mathbb{Z}/n\mathbb{Z}^*$. — Soit $x \in \mathbb{Z}$:

$$\begin{array}{rccc} & \text{pgcd}(n, x) = 1 & \Longrightarrow & \exists u, v \in \mathbb{Z},\ nu + xv = 1 \\ \overset{\text{mod } n}{\Longrightarrow} & \overline{n} \times \overline{u} + \overline{x} \times \overline{v} = \overline{1} & \Longrightarrow & \overline{0} \times \overline{u} + \overline{x} \times \overline{v} = \overline{1} \end{array}$$

Une autre caractérisation du pgcd

Thérème de Bezout

Soit $a, b \in \mathbb{Z}$ alors il existe $u, v \in \mathbb{Z}$ tels que :

$$au + bv = \text{pgcd}(a, b)$$

L'entier $\text{pgcd}(a, b)$ est l'unique entier (au signe près) qui

- est un diviseur commun de a et b,
- et qui est de la forme $au + bv$ avec $u, v \in \mathbb{Z}$.

Lien avec $\mathbb{Z}/n\mathbb{Z}^*$. — Soit $x \in \mathbb{Z}$:

$$\begin{aligned} & \text{pgcd}(n, x) = 1 && \implies && \exists u, v \in \mathbb{Z},\ nu + xv = 1 \\ \overset{\text{mod } n}{\implies} \quad & \overline{n} \times \overline{u} + \overline{x} \times \overline{v} = \overline{1} && \implies && \overline{0} \times \overline{u} + \overline{x} \times \overline{v} = \overline{1} \\ \implies \quad & \overline{x} \times \overline{v} = \overline{1} \end{aligned}$$

Le groupe $\mathbb{Z}/n\mathbb{Z}^*$ prend d'Euler

Le groupe $\mathbb{Z}/n\mathbb{Z}^*$ prend d'Euler

La fonction φ indicatrice d'Euler est définie par

$$\varphi(n) = \sharp\{x \in [1..n] \mid \text{pgcd}(x, n) = 1\},$$

Exemples

$\varphi(p) = p - 1$

$\varphi(pq) = (p-1)(q-1)$

Le groupe $\mathbb{Z}/n\mathbb{Z}^*$ prend d'Euler

La fonction φ indicatrice d'Euler est définie par

$$\varphi(n) = \sharp\{x \in [1..n] \mid \text{pgcd}(x, n) = 1\},$$

$$\Rightarrow \sharp\mathbb{Z}/n\mathbb{Z}^* = \varphi(n)$$

Exemples

$$\varphi(p) = p - 1$$

$$\varphi(pq) = (p-1)(q-1)$$

$$\sharp\mathbb{Z}/21\mathbb{Z}^* = (3-1)(7-1)$$

Le groupe $\mathbb{Z}/n\mathbb{Z}^*$ prend d'Euler

La fonction φ indicatrice d'Euler est définie par

$$\varphi(n) = \sharp\{x \in [1..n] \mid \text{pgcd}(x, n) = 1\},$$

$$\Rightarrow \sharp\mathbb{Z}/n\mathbb{Z}^* = \varphi(n)$$

Exemples

$\varphi(p) = p - 1$

$\varphi(pq) = (p-1)(q-1)$

$\sharp\mathbb{Z}/21\mathbb{Z}^* = (3-1)(7-1)$

Théorème d'Euler (1760)

Soit $n \geq 2$, un entier.

Le groupe $\mathbb{Z}/n\mathbb{Z}^*$ prend d'Euler

La fonction φ indicatrice d'Euler est définie par

$$\varphi(n) = \sharp\{x \in [1..n] \mid \text{pgcd}(x, n) = 1\},$$

$$\Rightarrow \sharp\mathbb{Z}/n\mathbb{Z}^* = \varphi(n)$$

Exemples

$$\varphi(p) = p - 1$$

$$\varphi(pq) = (p-1)(q-1)$$

$$\sharp\mathbb{Z}/21\mathbb{Z}^* = (3-1)(7-1)$$

Théorème d'Euler (1760)

Soit $n \geq 2$, un entier.

- **Dans** $\mathbb{Z}$. Pour tout $x \in \mathbb{Z}$ **premier** à n, on a

$$x^{\varphi(n)} \equiv 1 \pmod{n} \quad \text{ou encore} \quad n \text{ divise } \left(x^{\varphi(n)} - 1\right)$$

Le groupe $\mathbb{Z}/n\mathbb{Z}^*$ prend d'Euler

La fonction φ indicatrice d'Euler est définie par

$$\varphi(n) = \sharp\{x \in [1..n] \mid \text{pgcd}(x, n) = 1\},$$

$$\Rightarrow \sharp\mathbb{Z}/n\mathbb{Z}^* = \varphi(n)$$

Exemples

$$\varphi(p) = p - 1$$

$$\varphi(pq) = (p-1)(q-1)$$

$$\sharp\mathbb{Z}/21\mathbb{Z}^* = (3-1)(7-1)$$

Théorème d'Euler (1760)

Soit $n \geq 2$, un entier.

- **Dans** $\mathbb{Z}$. Pour tout $x \in \mathbb{Z}$ **premier** à n, on a

$$x^{\varphi(n)} \equiv 1 \pmod{n} \quad \text{ou encore} \quad n \text{ divise } \left(x^{\varphi(n)} - 1\right)$$

- **Dans** $\mathbb{Z}/n\mathbb{Z}$. $\forall \overline{x} \in \mathbb{Z}/n\mathbb{Z}^*, \quad \overline{x}^{\varphi(n)} = \overline{1}$.

Le Protocole RSA [Rivest, Shamir, Adleman, 1977]

Le Protocole RSA [Rivest, Shamir, Adleman, 1977]

Fonction asymétrique de RSA

On considère $n = p \times q$ avec p, q deux (grand) premiers distincts et $c \in \mathbb{Z}$ un entier inversible modulo $\varphi(n)$. La fonction asymétrique de RSA est

$$\begin{array}{rccc} C : & \mathbb{Z}/n\mathbb{Z}^* & \longrightarrow & \mathbb{Z}/n\mathbb{Z}^* \\ & m & \longmapsto & m^c \end{array}$$

Le Protocole RSA [Rivest, Shamir, Adleman, 1977]

Fonction asymétrique de RSA

On considère $n = p \times q$ avec p, q deux (grand) premiers distincts et $c \in \mathbb{Z}$ un entier inversible modulo $\varphi(n)$. La fonction asymétrique de RSA est

$$\begin{array}{rccc} C : & \mathbb{Z}/n\mathbb{Z}^* & \longrightarrow & \mathbb{Z}/n\mathbb{Z}^* \\ & m & \longmapsto & m^c \end{array}$$

Remarques

Le Protocole RSA [Rivest, Shamir, Adleman, 1977]

Fonction asymétrique de RSA

On considère $n = p \times q$ avec p, q deux (grand) premiers distincts et $c \in \mathbb{Z}$ un entier inversible modulo $\varphi(n)$. La fonction asymétrique de RSA est

$$\begin{array}{rccc} C : & \mathbb{Z}/n\mathbb{Z}^* & \longrightarrow & \mathbb{Z}/n\mathbb{Z}^* \\ & m & \longmapsto & m^c \end{array}$$

Remarques

- **Inefficacité.** L'entier n est public mais sa connaissance ne permet pas de retrouver les premiers p et q.

Le Protocole RSA [Rivest, Shamir, Adleman, 1977]

Fonction asymétrique de RSA

On considère $n = p \times q$ avec p, q deux (grand) premiers distincts et $c \in \mathbb{Z}$ un entier inversible modulo $\varphi(n)$. La fonction asymétrique de RSA est

$$\begin{array}{rccc} C : & \mathbb{Z}/n\mathbb{Z}^* & \longrightarrow & \mathbb{Z}/n\mathbb{Z}^* \\ & m & \longmapsto & m^c \end{array}$$

Remarques

- **Inefficacité.** L'entier n est public mais sa connaissance ne permet pas de retrouver les premiers p et q.
- L'**efficacité** de l'application de C reste encore à démontrer !

Le Protocole RSA [Rivest, Shamir, Adleman, 1977]

Fonction asymétrique de RSA

On considère $n = p \times q$ avec p, q deux (grand) premiers distincts et $c \in \mathbb{Z}$ un entier inversible modulo $\varphi(n)$. La fonction asymétrique de RSA est

$$\begin{array}{rccc} C : & \mathbb{Z}/n\mathbb{Z}^* & \longrightarrow & \mathbb{Z}/n\mathbb{Z}^* \\ & m & \longmapsto & m^c \end{array}$$

Remarques

- **Inefficacité.** L'entier n est public mais sa connaissance ne permet pas de retrouver les premiers p et q.
- L'**efficacité** de l'application de C reste encore à démontrer !
- La réciproque consiste donc à prendre la «racine c-ème» d'un élément de $\mathbb{Z}/n\mathbb{Z}^*$.

Le Protocole RSA — La Trappe

La trappe RSA

Soit d l'inverse de c modulo $\varphi(n)$. L'application de déchiffrement est

$$\begin{array}{rccc} D: & \mathbb{Z}/n\mathbb{Z}^* & \longrightarrow & \mathbb{Z}/n\mathbb{Z}^* \\ & m & \longmapsto & m^d \end{array}$$

Le Protocole RSA — La Trappe

La trappe RSA

Soit d l'inverse de c modulo $\varphi(n)$. L'application de déchiffrement est

$$\begin{array}{rccc} D: & \mathbb{Z}/n\mathbb{Z}^* & \longrightarrow & \mathbb{Z}/n\mathbb{Z}^* \\ & m & \longmapsto & m^d \end{array}$$

Par construction $c \times d = 1 + q\varphi(n)$ avec $q \in \mathbb{Z}$.

La trappe RSA

Soit d l'inverse de c modulo $\varphi(n)$. L'application de déchiffrement est

$$\begin{array}{rccc} D: & \mathbb{Z}/n\mathbb{Z}^* & \longrightarrow & \mathbb{Z}/n\mathbb{Z}^* \\ & m & \longmapsto & m^d \end{array}$$

Par construction $c \times d = 1 + q\varphi(n)$ avec $q \in \mathbb{Z}$.
Pour $m \in \mathbb{Z}/n\mathbb{Z}^*$ on a

$$\begin{aligned} D(C(m)) &= (m^c)^d = m^{cd} \\ &= m^{1+q\varphi(n)} = m \times \left(m^{\varphi(n)}\right)^q \\ &= m \times 1^q \qquad \text{[Euler]} \\ &= m \end{aligned}$$

Le Protocole RSA — Un cas d'école

Le Protocole RSA — Un cas d'école

Choisissons comme modulus RSA :

$$n = 77 = 7 \times 11 \quad \Rightarrow \quad \varphi(n) = (7-1)(11-1) = 60$$

Le Protocole RSA — Un cas d'école

Choisissons comme modulus RSA :

$$n = 77 = 7 \times 11 \quad \Rightarrow \quad \varphi(n) = (7-1)(11-1) = 60$$

Comme pgcd$(60, 13) = 1$, on peut choisir 13 comme clé de chiffrement/publique. On a alors :

$$c = 13 \quad \Rightarrow \quad d = c^{-1} \bmod 60 = 37$$

Le Protocole RSA — Un cas d'école

Choisissons comme modulus RSA :

$$n = 77 = 7 \times 11 \quad \Rightarrow \quad \varphi(n) = (7-1)(11-1) = 60$$

Comme $\text{pgcd}(60, 13) = 1$, on peut choisir 13 comme clé de chiffrement/publique. On a alors :

$$c = 13 \quad \Rightarrow \quad d = c^{-1} \bmod 60 = 37$$

et les applications de chiffrement et déchiffrement sont donc respectivement :

$$C(m) = m^{13} \pmod{77} \qquad D(m) = m^{37} \pmod{77}$$

Complexité des opérations entre entiers

Complexité des opérations entre entiers

Taille d'un entier

La taille d'un entier n, c'est-à-dire le nombre de ses chiffres binaires, vaut $1 + \lfloor \log_2(n) \rfloor$. L'ordre de grandeur est donc $O(\log(n))$.

Complexité des opérations entre entiers

Taille d'un entier

La taille d'un entier n, c'est-à-dire le nombre de ses chiffres binaires, vaut $1 + \lfloor \log_2(n) \rfloor$. L'ordre de grandeur est donc $O(\log(n))$.

Coût des opérations élémentaires entre entiers

Complexité des opérations entre entiers

Taille d'un entier

La taille d'un entier n, c'est-à-dire le nombre de ses chiffres binaires, vaut $1 + \lfloor \log_2(n) \rfloor$. L'ordre de grandeur est donc $O(\log(n))$.

Coût des opérations élémentaires entre entiers

- L'addition de deux entiers $\leq n$: $O(\log(n))$

Complexité des opérations entre entiers

Taille d'un entier

La taille d'un entier n, c'est-à-dire le nombre de ses chiffres binaires, vaut $1 + \lfloor \log_2(n) \rfloor$. L'ordre de grandeur est donc $O(\log(n))$.

Coût des opérations élémentaires entre entiers

- L'addition de deux entiers $\leq n$: $O(\log(n))$
- Le produit de deux entiers $\leq n$: $O\left(\log(n)^2\right)$

Complexité des opérations entre entiers

Taille d'un entier

La taille d'un entier n, c'est-à-dire le nombre de ses chiffres binaires, vaut $1 + \lfloor \log_2(n) \rfloor$. L'ordre de grandeur est donc $O(\log(n))$.

Coût des opérations élémentaires entre entiers

- L'addition de deux entiers $\leq n$: $O(\log(n))$
- Le produit de deux entiers $\leq n$: $O\left(\log(n)^2\right)$
- Le pgcd de deux entiers $\leq n$: $O\left(\log(n)^2\right)$

Complexité des opérations entre entiers

Taille d'un entier

La taille d'un entier n, c'est-à-dire le nombre de ses chiffres binaires, vaut $1 + \lfloor \log_2(n) \rfloor$. L'ordre de grandeur est donc $O(\log(n))$.

Coût des opérations élémentaires entre entiers

- L'addition de deux entiers $\leq n$: $O(\log(n))$
- Le produit de deux entiers $\leq n$: $O\left(\log(n)^2\right)$
- Le pgcd de deux entiers $\leq n$: $O\left(\log(n)^2\right)$
- L'exponentiation $\overline{x} \mapsto \overline{x}^{\epsilon}$ modulo n : $O\left(\log(n)^2 \log(\epsilon)\right)$

Complexité des opérations entre entiers

Taille d'un entier

La taille d'un entier n, c'est-à-dire le nombre de ses chiffres binaires, vaut $1 + \lfloor \log_2(n) \rfloor$. L'ordre de grandeur est donc $O(\log(n))$.

Coût des opérations élémentaires entre entiers

- L'addition de deux entiers $\leq n$: $O(\log(n))$
- Le produit de deux entiers $\leq n$: $O\left(\log(n)^2\right)$
- Le pgcd de deux entiers $\leq n$: $O\left(\log(n)^2\right)$
- L'exponentiation $\overline{x} \mapsto \overline{x}^{\epsilon}$ modulo n : $O\left(\log(n)^2 \log(\epsilon)\right)$
- Décider si n est premier : $O\left(\log(n)^3\right)$

Complexité des opérations entre entiers

Taille d'un entier

La taille d'un entier n, c'est-à-dire le nombre de ses chiffres binaires, vaut $1 + \lfloor \log_2(n) \rfloor$. L'ordre de grandeur est donc $O(\log(n))$.

Coût des opérations élémentaires entre entiers

- L'addition de deux entiers $\leq n$: $O(\log(n))$
- Le produit de deux entiers $\leq n$: $O\left(\log(n)^2\right)$
- Le pgcd de deux entiers $\leq n$: $O\left(\log(n)^2\right)$
- L'exponentiation $\overline{x} \mapsto \overline{x}^{\epsilon}$ modulo n : $O\left(\log(n)^2 \log(\epsilon)\right)$
- Décider si n est premier : $O\left(\log(n)^3\right)$
- factoriser un entier n : naïvement $\sqrt{n}$. Aucun algorithme polynomial connu.

Exponentiation dichotomique — Exemple

Exponentiation dichotomique — Exemple

Calcul du chiffrement (public) $C(x) = x^{13}$.

Exponentiation dichotomique — Exemple

Calcul du chiffrement (public) $C(x) = x^{13}$.

- On écrit 13 en base 2, $13 = 8 + 4 + 1 = 2^3 + 2^2 + 2^0$.

Exponentiation dichotomique — Exemple

Calcul du chiffrement (public) $C(x) = x^{13}$.

- On écrit 13 en base 2, $13 = 8 + 4 + 1 = 2^3 + 2^2 + 2^0$.
- On décompose :

$$x^{13} = x^{8+4+1} = x^8 \times x^4 \times x = x^{2^3} \times x^{2^2} \times x^{2^0} \qquad (\star)$$

Exponentiation dichotomique — Exemple

Calcul du chiffrement (public) $C(x) = x^{13}$.

- On écrit 13 en base 2, $13 = 8 + 4 + 1 = 2^3 + 2^2 + 2^0$.
- On décompose :

$$x^{13} = x^{8+4+1} = x^8 \times x^4 \times x = x^{2^3} \times x^{2^2} \times x^{2^0} \qquad (\star)$$

- Comme $\left(x^{2^i}\right)^2 = x^{2^{i+1}}$, trois carrés successifs suffisent à calculer les termes du produit $(\star)$:

$$x \quad \text{au carré} \rightsquigarrow \quad x^2 \quad \text{au carré} \rightsquigarrow \quad x^4 \quad \text{au carré} \rightsquigarrow \quad x^8$$

Exponentiation dichotomique — Exemple

Calcul du chiffrement (public) $C(x) = x^{13}$.

- On écrit 13 en base 2, $13 = 8 + 4 + 1 = 2^3 + 2^2 + 2^0$.
- On décompose :

$$x^{13} = x^{8+4+1} = x^8 \times x^4 \times x = x^{2^3} \times x^{2^2} \times x^{2^0} \qquad (\star)$$

- Comme $\left(x^{2^i}\right)^2 = x^{2^{i+1}}$, trois carrés successifs suffisent à calculer les termes du produit $(\star)$:

$$x \quad \text{au carré} \rightsquigarrow \quad x^2 \quad \text{au carré} \rightsquigarrow \quad x^4 \quad \text{au carré} \rightsquigarrow \quad x^8$$

- On calcule le produit $(\star)$. Total : $5 = 3 + 2$ produits au lieu de $12 = 13 - 1$ naïvement.

Exponentiation dichotomique — L'algorithme

Exponentiation dichotomique — L'algorithme

- **Entrée** x, ϵ

Exponentiation dichotomique — L'algorithme

- **Entrée** x, ϵ
- **Initialisation**
  - $(r, c, e) \leftarrow (1, x, \epsilon)$

Exponentiation dichotomique — L'algorithme

- **Entrée** x, ϵ
- **Initialisation**
  - $(r, c, e) \leftarrow (1, x, \epsilon)$
- Tant que $e \neq 0$ répéter

Exponentiation dichotomique — L'algorithme

- **Entrée** x, ϵ
- **Initialisation**
  - $(r, c, e) \leftarrow (1, x, \epsilon)$
- Tant que $e \neq 0$ répéter
  - Si e pair

    $e \leftarrow e \div 2$

Exponentiation dichotomique — L'algorithme

- **Entrée** x, ϵ
- **Initialisation**
  - $(r, c, e) \leftarrow (1, x, \epsilon)$
- Tant que $e \neq 0$ répéter
  - Si e pair
    $e \leftarrow e \div 2$
  - Sinon
    $e \leftarrow (e - 1) \div 2$
    $r \leftarrow r \times c$

Exponentiation dichotomique — L'algorithme

- **Entrée** x, ϵ
- **Initialisation**
  - $(r, c, e) \leftarrow (1, x, \epsilon)$
- Tant que $e \neq 0$ répéter
  - Si e pair
    $e \leftarrow e \div 2$
  - Sinon
    $e \leftarrow (e - 1) \div 2$
    $r \leftarrow r \times c$
  - $c \leftarrow c^2$

Exponentiation dichotomique — L'algorithme

- **Entrée** x, ϵ
- **Initialisation**
  - $(r, c, e) \leftarrow (1, x, \epsilon)$
- Tant que $e \neq 0$ répéter
  - Si e pair
    $e \leftarrow e \div 2$
  - Sinon
    $e \leftarrow (e-1) \div 2$
    $r \leftarrow r \times c$
  - $c \leftarrow c^2$
- **Retourner** r $\qquad [r = x^\epsilon]$

Algorithme d'Euclide «classique»

Algorithme d'Euclide «classique»

Calcul de la clé de déchiffrement (privée)

$$d = c^{-1} \bmod \varphi(n) = 13^{-1} \bmod 60$$

Algorithme d'Euclide «classique»

Calcul de la clé de déchiffrement (privée)

$$d = c^{-1} \bmod \varphi(n) = 13^{-1} \bmod 60$$

- On part de $r_0 = 60$ et $r_1 = 13$.

Algorithme d'Euclide «classique»

Calcul de la clé de déchiffrement (privée)

$$d = c^{-1} \bmod \varphi(n) = 13^{-1} \bmod 60$$

- On part de $r_0 = 60$ et $r_1 = 13$.
- On calcule la suite des restes de l'algorithme d'Euclide

$$\begin{aligned} 60 &= 13 \times 4 + 8 & r_0 &= r_1 \times q_2 + r_2 \\ 13 &= 8 \times 1 + 5 & r_1 &= r_2 \times q_3 + r_3 \\ 8 &= 5 \times 1 + 3 & r_2 &= r_3 \times q_4 + r_4 \\ 5 &= 3 \times 1 + 2 & r_3 &= r_4 \times q_5 + r_5 \\ 3 &= 2 \times 1 + 1 & r_4 &= r_5 \times q_6 + r_6 \\ 2 &= 1 \times 2 + 0 & r_5 &= r_6 \times q_7 + r_7 \end{aligned}$$

Algorithme d'Euclide «classique»

Calcul de la clé de déchiffrement (privée)

$$d = c^{-1} \bmod \varphi(n) = 13^{-1} \bmod 60$$

- On part de $r_0 = 60$ et $r_1 = 13$.
- On calcule la suite des restes de l'algorithme d'Euclide

$$\begin{aligned} 60 &= 13 \times 4 + 8 & r_0 &= r_1 \times q_2 + r_2 \\ 13 &= 8 \times 1 + 5 & r_1 &= r_2 \times q_3 + r_3 \\ 8 &= 5 \times 1 + 3 & r_2 &= r_3 \times q_4 + r_4 \\ 5 &= 3 \times 1 + 2 & r_3 &= r_4 \times q_5 + r_5 \\ 3 &= 2 \times 1 + 1 & r_4 &= r_5 \times q_6 + r_6 \\ 2 &= 1 \times 2 + 0 & r_5 &= r_6 \times q_7 + r_7 \end{aligned}$$

- $r_7 = 0$ et $r_6 \neq 0 \Rightarrow r_6 = 1 = \text{pgcd}(60, 13)$.

Algorithme d'Euclide «classique»

Calcul de la clé de déchiffrement (privée)

$$d = c^{-1} \bmod \varphi(n) = 13^{-1} \bmod 60$$

- On part de $r_0 = 60$ et $r_1 = 13$.
- On calcule la suite des restes de l'algorithme d'Euclide

$$\begin{aligned} 60 &= 13 \times 4 + 8 & r_0 &= r_1 \times q_2 + r_2 \\ 13 &= 8 \times 1 + 5 & r_1 &= r_2 \times q_3 + r_3 \\ 8 &= 5 \times 1 + 3 & r_2 &= r_3 \times q_4 + r_4 \\ 5 &= 3 \times 1 + 2 & r_3 &= r_4 \times q_5 + r_5 \\ 3 &= 2 \times 1 + 1 & r_4 &= r_5 \times q_6 + r_6 \\ 2 &= 1 \times 2 + 0 & r_5 &= r_6 \times q_7 + r_7 \end{aligned}$$

- $r_7 = 0$ et $r_6 \neq 0 \Rightarrow r_6 = 1 = \text{pgcd}(60, 13)$.
- Comment calculer des coefficients de Bezout u, v tels que $60u + 13v = 1$?

Algorithme d'Euclide «Bezout enrichi»

Algorithme d'Euclide «Bezout enrichi»

- **Idée :** écrire tous les restes successifs r_i sous la forme $r_i = 60u_i + 13v_i$.

Algorithme d'Euclide «Bezout enrichi»

- **Idée :** écrire tous les restes successifs r_i sous la forme $r_i = 60u_i + 13v_i$.
- C'est facile pour r_0, r_1 ! La preuve :

$$r_0 = 60 = 60 \times 1 + 13 \times 0 \quad r_1 = 13 = 60 \times 0 + 13 \times 1$$

Algorithme d'Euclide «Bezout enrichi»

- **Idée :** écrire tous les restes successifs r_i sous la forme $r_i = 60u_i + 13v_i$.
- C'est facile pour r_0, r_1 ! La preuve :

$$r_0 = 60 = 60 \times 1 + 13 \times 0 \quad r_1 = 13 = 60 \times 0 + 13 \times 1$$

- Si on sait le faire pour r_i, r_{i+1}, on sait le faire pour r_{i+2} :

$$\begin{cases} r_i = 60u_i + 13v_i \\ r_{i+1} = 60u_{i+1} + 13v_{i+1} \\ r_{i+2} = r_i - q_{i+2}r_{i+1} \end{cases}$$

$$\begin{array}{c|c} r_i & r_{i+1} \\ \hline & q_{i+2} \\ r_{i+2} & \end{array}$$

$$\Longrightarrow \quad r_{i+2} = 60\underbrace{(u_i - q_{i+2}u_{i+1})}_{u_{i+2}} + 13\underbrace{(v_i - q_{i+2}v_{i+1})}_{v_{i+2}}$$

Clé de déchiffrement de RSA $(77, 13)$

i	r_i	u_i	q_i	v_i	Relations de Bezout

Clé de déchiffrement de RSA $(77, 13)$

i	r_i	u_i	q_i	v_i	Relations de Bezout
0	60	1		0	$60 = 60 \times 1 + 13 \times 0$
1	13	0		1	$13 = 60 \times 0 + 13 \times 1$

Clé de déchiffrement de RSA $(77, 13)$

i	r_i	u_i	q_i	v_i	Relations de Bezout
0	60	1		0	$60 = 60 \times 1 + 13 \times 0$
1	13	0		1	$13 = 60 \times 0 + 13 \times 1$
2	8	1	4	-4	$8 = 60 \times 1 + 13 \times (-4)$

Clé de déchiffrement de RSA $(77, 13)$

i	r_i	u_i	q_i	v_i	Relations de Bezout
0	60	1		0	$60 = 60 \times 1 + 13 \times 0$
1	13	0		1	$13 = 60 \times 0 + 13 \times 1$
2	8	1	4	-4	$8 = 60 \times 1 + 13 \times (-4)$
3	5	-1	1	5	$5 = 60 \times (-1) + 13 \times 5$

Clé de déchiffrement de RSA $(77, 13)$

i	r_i	u_i	q_i	v_i	Relations de Bezout
0	60	1		0	$60 = 60 \times 1 + 13 \times 0$
1	13	0		1	$13 = 60 \times 0 + 13 \times 1$
2	8	1	4	-4	$8 = 60 \times 1 + 13 \times (-4)$
3	5	-1	1	5	$5 = 60 \times (-1) + 13 \times 5$
4	3	2	1	-9	$3 = 60 \times 2 + 13 \times (-9)$

Clé de déchiffrement de RSA $(77, 13)$

i	r_i	u_i	q_i	v_i	Relations de Bezout
0	60	1		0	$60 = 60 \times 1 + 13 \times 0$
1	13	0		1	$13 = 60 \times 0 + 13 \times 1$
2	8	1	4	-4	$8 = 60 \times 1 + 13 \times (-4)$
3	5	-1	1	5	$5 = 60 \times (-1) + 13 \times 5$
4	3	2	1	-9	$3 = 60 \times 2 + 13 \times (-9)$
5	2	-3	1	14	$2 = 60 \times (-3) + 13 \times 14$

Clé de déchiffrement de RSA $(77, 13)$

i	r_i	u_i	q_i	v_i	Relations de Bezout
0	60	1		0	$60 = 60 \times 1 + 13 \times 0$
1	13	0		1	$13 = 60 \times 0 + 13 \times 1$
2	8	1	4	-4	$8 = 60 \times 1 + 13 \times (-4)$
3	5	-1	1	5	$5 = 60 \times (-1) + 13 \times 5$
4	3	2	1	-9	$3 = 60 \times 2 + 13 \times (-9)$
5	2	-3	1	14	$2 = 60 \times (-3) + 13 \times 14$
6	1	5	1	-23	$1 = 60 \times 5 + 13 \times (-23)$

Clé de déchiffrement de RSA $(77, 13)$

i	r_i	u_i	q_i	v_i	Relations de Bezout
0	60	1		0	$60 = 60 \times 1 + 13 \times 0$
1	13	0		1	$13 = 60 \times 0 + 13 \times 1$
2	8	1	4	-4	$8 = 60 \times 1 + 13 \times (-4)$
3	5	-1	1	5	$5 = 60 \times (-1) + 13 \times 5$
4	3	2	1	-9	$3 = 60 \times 2 + 13 \times (-9)$
5	2	-3	1	14	$2 = 60 \times (-3) + 13 \times 14$
6	1	5	1	-23	$1 = 60 \times 5 + 13 \times (-23)$
7	0	-13	2	60	$0 = 60 \times (-13) + 13 \times 60$

Clé de déchiffrement de RSA $(77, 13)$

i	r_i	u_i	q_i	v_i	Relations de Bezout
0	60	1		0	$60 = 60 \times 1 + 13 \times 0$
1	13	0		1	$13 = 60 \times 0 + 13 \times 1$
2	8	1	4	-4	$8 = 60 \times 1 + 13 \times (-4)$
3	5	-1	1	5	$5 = 60 \times (-1) + 13 \times 5$
4	3	2	1	-9	$3 = 60 \times 2 + 13 \times (-9)$
5	2	-3	1	14	$2 = 60 \times (-3) + 13 \times 14$
6	1	5	1	-23	$1 = 60 \times 5 + 13 \times (-23)$
7	0	-13	2	60	$0 = 60 \times (-13) + 13 \times 60$

L'identité de Bezout rouge donne modulo 60 :

Clé de déchiffrement de RSA $(77, 13)$

i	r_i	u_i	q_i	v_i	Relations de Bezout
0	60	1		0	$60 = 60 \times 1 + 13 \times 0$
1	13	0		1	$13 = 60 \times 0 + 13 \times 1$
2	8	1	4	-4	$8 = 60 \times 1 + 13 \times (-4)$
3	5	-1	1	5	$5 = 60 \times (-1) + 13 \times 5$
4	3	2	1	-9	$3 = 60 \times 2 + 13 \times (-9)$
5	2	-3	1	14	$2 = 60 \times (-3) + 13 \times 14$
6	1	5	1	-23	$1 = 60 \times 5 + 13 \times (-23)$
7	0	-13	2	60	$0 = 60 \times (-13) + 13 \times 60$

L'identité de Bezout rouge donne modulo 60 :

$$\overline{1} = \overline{60} \times \overline{5} + \overline{13} \times \overline{-23} = \overline{0} \times \overline{5} + \overline{13} \times \overline{-23} = \overline{13} \times \overline{-23}$$

Clé de déchiffrement de RSA $(77, 13)$

i	r_i	u_i	q_i	v_i	Relations de Bezout
0	60	1		0	$60 = 60 \times 1 + 13 \times 0$
1	13	0		1	$13 = 60 \times 0 + 13 \times 1$
2	8	1	4	-4	$8 = 60 \times 1 + 13 \times (-4)$
3	5	-1	1	5	$5 = 60 \times (-1) + 13 \times 5$
4	3	2	1	-9	$3 = 60 \times 2 + 13 \times (-9)$
5	2	-3	1	14	$2 = 60 \times (-3) + 13 \times 14$
6	1	5	1	-23	$1 = 60 \times 5 + 13 \times (-23)$
7	0	-13	2	60	$0 = 60 \times (-13) + 13 \times 60$

L'identité de Bezout rouge donne modulo 60 :

$$\overline{1} = \overline{60} \times \overline{5} + \overline{13} \times \overline{-23} = \overline{0} \times \overline{5} + \overline{13} \times \overline{-23} = \overline{13} \times \overline{-23}$$

Ainsi $\overline{13} \in \mathbb{Z}/60\mathbb{Z}^*$ et $\overline{13}^{-1} = \overline{-23} = \overline{37}$.

Algorithme d'Euclide «étendu»

Algorithme d'Euclide «étendu»

- **Entrée** $a, b \in \mathbb{Z}$

Algorithme d'Euclide «étendu»

- **Entrée** $a, b \in \mathbb{Z}$
- **Initialisation**
  - $(r_0, u_0, v_0) \leftarrow (a, 1, 0)$ $\quad [r_0 = au_0 + bv_0]$
  - $(r_1, u_1, v_1) \leftarrow (b, 0, 1)$ $\quad [r_1 = au_1 + bv_1]$

Algorithme d'Euclide «étendu»

- **Entrée** $a, b \in \mathbb{Z}$
- **Initialisation**
  - $(r_0, u_0, v_0) \leftarrow (a, 1, 0)$ $\quad [r_0 = au_0 + bv_0]$
  - $(r_1, u_1, v_1) \leftarrow (b, 0, 1)$ $\quad [r_1 = au_1 + bv_1]$
- Tant que $r_1 \neq 0$, répéter

Algorithme d'Euclide «étendu»

- **Entrée** $a, b \in \mathbb{Z}$
- **Initialisation**
  - $(r_0, u_0, v_0) \leftarrow (a, 1, 0)$ $\quad [r_0 = au_0 + bv_0]$
  - $(r_1, u_1, v_1) \leftarrow (b, 0, 1)$ $\quad [r_1 = au_1 + bv_1]$
- Tant que $r_1 \neq 0$, répéter
  - $(r_{\text{aux}}, q_{\text{aux}}) \leftarrow (r_0 \bmod r_1, r_0 \div r_1)$ $\quad [r_{\text{aux}} = r_0 - q_{\text{aux}} r_1]$

Algorithme d'Euclide «étendu»

- **Entrée** $a, b \in \mathbb{Z}$
- **Initialisation**
  - $(r_0, u_0, v_0) \leftarrow (a, 1, 0)$ $\quad [r_0 = au_0 + bv_0]$
  - $(r_1, u_1, v_1) \leftarrow (b, 0, 1)$ $\quad [r_1 = au_1 + bv_1]$
- Tant que $r_1 \neq 0$, répéter
  - $(r_{\text{aux}}, q_{\text{aux}}) \leftarrow (r_0 \bmod r_1, r_0 \div r_1)$ $\quad [r_{\text{aux}} = r_0 - q_{\text{aux}} r_1]$
  - $u_{\text{aux}} \leftarrow u_0 - q_{\text{aux}} u_1$

Algorithme d'Euclide «étendu»

- **Entrée** $a, b \in \mathbb{Z}$
- **Initialisation**
  - $(r_0, u_0, v_0) \leftarrow (a, 1, 0)$ $\quad [r_0 = au_0 + bv_0]$
  - $(r_1, u_1, v_1) \leftarrow (b, 0, 1)$ $\quad [r_1 = au_1 + bv_1]$
- Tant que $r_1 \neq 0$, répéter
  - $(r_{\text{aux}}, q_{\text{aux}}) \leftarrow (r_0 \bmod r_1, r_0 \div r_1)$ $\quad [r_{\text{aux}} = r_0 - q_{\text{aux}} r_1]$
  - $u_{\text{aux}} \leftarrow u_0 - q_{\text{aux}} u_1$
  - $v_{\text{aux}} \leftarrow v_0 - q_{\text{aux}} v_1$

Algorithme d'Euclide «étendu»

- **Entrée** $a, b \in \mathbb{Z}$
- **Initialisation**
  - $(r_0, u_0, v_0) \leftarrow (a, 1, 0)$ $\quad [r_0 = au_0 + bv_0]$
  - $(r_1, u_1, v_1) \leftarrow (b, 0, 1)$ $\quad [r_1 = au_1 + bv_1]$
- Tant que $r_1 \neq 0$, répéter
  - $(r_{\text{aux}}, q_{\text{aux}}) \leftarrow (r_0 \bmod r_1, r_0 \div r_1)$ $\quad [r_{\text{aux}} = r_0 - q_{\text{aux}} r_1]$
  - $u_{\text{aux}} \leftarrow u_0 - q_{\text{aux}} u_1$
  - $v_{\text{aux}} \leftarrow v_0 - q_{\text{aux}} v_1$
  - $(r_0, u_0, v_0) \leftarrow (r_1, u_1, v_1)$ $\quad [r_{\text{aux}} = au_{\text{aux}} + bv_{\text{aux}}]$

Algorithme d'Euclide «étendu»

- **Entrée** $a, b \in \mathbb{Z}$
- **Initialisation**
  - $(r_0, u_0, v_0) \leftarrow (a, 1, 0)$ $\quad [r_0 = au_0 + bv_0]$
  - $(r_1, u_1, v_1) \leftarrow (b, 0, 1)$ $\quad [r_1 = au_1 + bv_1]$
- Tant que $r_1 \neq 0$, répéter
  - $(r_{\text{aux}}, q_{\text{aux}}) \leftarrow (r_0 \bmod r_1, r_0 \div r_1)$ $\quad [r_{\text{aux}} = r_0 - q_{\text{aux}} r_1]$
  - $u_{\text{aux}} \leftarrow u_0 - q_{\text{aux}} u_1$
  - $v_{\text{aux}} \leftarrow v_0 - q_{\text{aux}} v_1$
  - $(r_0, u_0, v_0) \leftarrow (r_1, u_1, v_1)$ $\quad [r_{\text{aux}} = au_{\text{aux}} + bv_{\text{aux}}]$
  - $(r_1, u_1, v_1) \leftarrow (r_{\text{aux}}, u_{\text{aux}}, v_{\text{aux}})$

Algorithme d'Euclide «étendu»

- **Entrée** $a, b \in \mathbb{Z}$
- **Initialisation**
  - $(r_0, u_0, v_0) \leftarrow (a, 1, 0)$ $\quad [r_0 = au_0 + bv_0]$
  - $(r_1, u_1, v_1) \leftarrow (b, 0, 1)$ $\quad [r_1 = au_1 + bv_1]$
- Tant que $r_1 \neq 0$, répéter
  - $(r_{\text{aux}}, q_{\text{aux}}) \leftarrow (r_0 \bmod r_1, r_0 \div r_1)$ $\quad [r_{\text{aux}} = r_0 - q_{\text{aux}} r_1]$
  - $u_{\text{aux}} \leftarrow u_0 - q_{\text{aux}} u_1$
  - $v_{\text{aux}} \leftarrow v_0 - q_{\text{aux}} v_1$
  - $(r_0, u_0, v_0) \leftarrow (r_1, u_1, v_1)$ $\quad [r_{\text{aux}} = au_{\text{aux}} + bv_{\text{aux}}]$
  - $(r_1, u_1, v_1) \leftarrow (r_{\text{aux}}, u_{\text{aux}}, v_{\text{aux}})$
- **Retourner** (r_0, u_0, u_0) $\quad [r_0 = \text{pgcd}(a, b) = au_0 + bv_0]$

Un secret bien gardé ? L'indicateur d'Euler $\varphi(n)$

Un secret bien gardé ? L'indicateur d'Euler $\varphi(n)$

Qui sait...

Qui sait efficacement calculer $\varphi(n)$ sait efficacement calculer p et q.

Un secret bien gardé ? L'indicateur d'Euler $\varphi(n)$

Qui sait...

Qui sait efficacement calculer $\varphi(n)$ sait efficacement calculer p et q.

La somme $p+q$ et le produit $p \times q$ s'expriment en fonction de n et $\varphi(n)$:

Un secret bien gardé ? L'indicateur d'Euler $\varphi(n)$

Qui sait...

Qui sait efficacement calculer $\varphi(n)$ sait efficacement calculer p et q.

La somme $p+q$ et le produit $p \times q$ s'expriment en fonction de n et $\varphi(n)$:

$$\begin{cases} n = p \times q \\ \varphi(n) = (p-1) \times (q-1) \end{cases}$$

Un secret bien gardé ? L'indicateur d'Euler $\varphi(n)$

Qui sait...

Qui sait efficacement calculer $\varphi(n)$ sait efficacement calculer p et q.

La somme $p+q$ et le produit $p \times q$ s'expriment en fonction de n et $\varphi(n)$:

$$\begin{cases} n = p \times q \\ \varphi(n) = (p-1) \times (q-1) \end{cases} \Longrightarrow \begin{cases} p \times q = n \\ p + q = n - \varphi(n) + 1 \end{cases}$$

Un secret bien gardé ? L'indicateur d'Euler $\varphi(n)$

Qui sait...

Qui sait efficacement calculer $\varphi(n)$ sait efficacement calculer p et q.

La somme $p+q$ et le produit $p \times q$ s'expriment en fonction de n et $\varphi(n)$:

$$\begin{cases} n = p \times q \\ \varphi(n) = (p-1) \times (q-1) \end{cases} \Longrightarrow \begin{cases} p \times q = n \\ p + q = n - \varphi(n) + 1 \end{cases}$$

Donc p et q sont les racines du trinôme :

Un secret bien gardé ? L'indicateur d'Euler $\varphi(n)$

Qui sait...

Qui sait efficacement calculer $\varphi(n)$ sait efficacement calculer p et q.

La somme $p+q$ et le produit $p \times q$ s'expriment en fonction de n et $\varphi(n)$:

$$\begin{cases} n = p \times q \\ \varphi(n) = (p-1) \times (q-1) \end{cases} \Longrightarrow \begin{cases} p \times q = n \\ p + q = n - \varphi(n) + 1 \end{cases}$$

Donc p et q sont les racines du trinôme :

$$X^2 - (n - \varphi(n) + 1)X + n = (X - p)(X - q)$$

Un secret bien gardé ? La clé secrète d

Un secret bien gardé ? La clé secrète d

Qui sait...

Qui sait efficacement calculer la clé d sait efficacement calculer p et q avec une bonne probabilité de succès.

Un secret bien gardé ? La clé secrète d

Qui sait...

Qui sait efficacement calculer la clé d sait efficacement calculer p et q avec une bonne probabilité de succès.

- **Entrée** n, c, d

Un secret bien gardé ? La clé secrète d

Qui sait...

Qui sait efficacement calculer la clé d sait efficacement calculer p et q avec une bonne probabilité de succès.

- **Entrée** n, c, d
- $e \leftarrow c \times d - 1$;
  tant que e est pair répéter $e \leftarrow e \div 2$ $\quad [cd - 1 = 2^{\alpha} \times e]$

Un secret bien gardé ? La clé secrète d

Qui sait. . .

Qui sait efficacement calculer la clé d sait efficacement calculer p et q avec une bonne probabilité de succès.

- **Entrée** n, c, d
- $e \leftarrow c \times d - 1$;
  tant que e est pair répéter $e \leftarrow e \div 2$ $\quad [cd - 1 = 2^\alpha \times e]$
- tirer x au hasard dans $[2..n]$

Un secret bien gardé ? La clé secrète d

Qui sait. . .

Qui sait efficacement calculer la clé d sait efficacement calculer p et q avec une bonne probabilité de succès.

- **Entrée** n, c, d
- $e \leftarrow c \times d - 1$;
  tant que e est pair répéter $e \leftarrow e \div 2$ $\quad [cd - 1 = 2^\alpha \times e]$
- tirer x au hasard dans $[2..n]$
- $y \leftarrow x^e \bmod n$; $z \leftarrow y$

Un secret bien gardé ? La clé secrète d

Qui sait. . .

Qui sait efficacement calculer la clé d sait efficacement calculer p et q avec une bonne probabilité de succès.

- **Entrée** n, c, d
- $e \leftarrow c \times d - 1$;
  tant que e est pair répéter $e \leftarrow e \div 2$ $\quad [cd - 1 = 2^\alpha \times e]$
- tirer x au hasard dans $[2..n]$
- $y \leftarrow x^e \bmod n$; $z \leftarrow y$
- tant que $z \neq 1$ répéter

Un secret bien gardé ? La clé secrète d

Qui sait. . .

Qui sait efficacement calculer la clé d sait efficacement calculer p et q avec une bonne probabilité de succès.

- **Entrée** n, c, d
- $e \leftarrow c \times d - 1$;
  tant que e est pair répéter $e \leftarrow e \div 2$ $\quad [cd - 1 = 2^\alpha \times e]$
- tirer x au hasard dans $[2..n]$
- $y \leftarrow x^e \bmod n$; $z \leftarrow y$
- tant que $z \neq 1$ répéter
  - $y \leftarrow z$; $z \leftarrow z^2$

Un secret bien gardé ? La clé secrète d

Qui sait. . .

Qui sait efficacement calculer la clé d sait efficacement calculer p et q avec une bonne probabilité de succès.

- **Entrée** n, c, d
- $e \leftarrow c \times d - 1$;
  tant que e est pair répéter $e \leftarrow e \div 2$ $\quad [cd - 1 = 2^\alpha \times e]$
- tirer x au hasard dans $[2..n]$
- $y \leftarrow x^e \bmod n$; $z \leftarrow y$
- tant que $z \neq 1$ répéter
  - $y \leftarrow z$; $z \leftarrow z^2$
- Si $y = -1$ retour au tirage de x $\quad [y^2 \bmod n = 1]$

Un secret bien gardé ? La clé secrète d

Qui sait. . .

Qui sait efficacement calculer la clé d sait efficacement calculer p et q avec une bonne probabilité de succès.

- **Entrée** n, c, d
- $e \leftarrow c \times d - 1$;
  tant que e est pair répéter $e \leftarrow e \div 2$ $\quad [cd - 1 = 2^\alpha \times e]$
- tirer x au hasard dans $[2..n]$
- $y \leftarrow x^e \bmod n$; $z \leftarrow y$
- tant que $z \neq 1$ répéter
  - $y \leftarrow z$; $z \leftarrow z^2$
- Si $y = -1$ retour au tirage de x $\quad [y^2 \bmod n = 1]$
- **Retourner** $\text{pgcd}(n, y - 1), \text{pgcd}(n, y + 1)$

Primalité

Primalité

Th. des nombres premiers [Hadamard & La Vallée Poussin, 1896]

Entre 1 et n, la proportion de nombres premiers est de l'ordre de $1/\ln(n)$ quand n grandit.

Primalité

Th. des nombres premiers [Hadamard & La Vallée Poussin, 1896]

Entre 1 et n, la proportion de nombres premiers est de l'ordre de $1/\ln(n)$ quand n grandit.

$\Rightarrow$ Les premiers sont assez nombreux.

Primalité

Th. des nombres premiers [Hadamard & La Vallée Poussin, 1896]

Entre 1 et n, la proportion de nombres premiers est de l'ordre de $1/\ln(n)$ quand n grandit.

$\Rightarrow$ Les premiers sont assez nombreux.

Prime is P [Agrawal-Kayal-Saxena, 2002]

Il existe un algorithme polynomial, déterministe permettant de tester la primalité d'un entier.

Primalité

Th. des nombres premiers [Hadamard & La Vallée Poussin, 1896]

Entre 1 et n, la proportion de nombres premiers est de l'ordre de $1/\ln(n)$ quand n grandit.

$\Rightarrow$ Les premiers sont assez nombreux.

Prime is P [Agrawal-Kayal-Saxena, 2002]

Il existe un algorithme polynomial, déterministe permettant de tester la primalité d'un entier.

Complexité sextique $\Rightarrow$ Algorithmes polynomial, probabilistes

Primalité

Th. des nombres premiers [Hadamard & La Vallée Poussin, 1896]

Entre 1 et n, la proportion de nombres premiers est de l'ordre de $1/\ln(n)$ quand n grandit.

$\Rightarrow$ Les premiers sont assez nombreux.

Prime is P [Agrawal-Kayal-Saxena, 2002]

Il existe un algorithme polynomial, déterministe permettant de tester la primalité d'un entier.

Complexité sextique $\Rightarrow$ Algorithmes polynomial, probabilistes

- Test de Miller-Rabin

Primalité

Th. des nombres premiers [Hadamard & La Vallée Poussin, 1896]

Entre 1 et n, la proportion de nombres premiers est de l'ordre de $1/\ln(n)$ quand n grandit.

$\Rightarrow$ Les premiers sont assez nombreux.

Prime is P [Agrawal-Kayal-Saxena, 2002]

Il existe un algorithme polynomial, déterministe permettant de tester la primalité d'un entier.

Complexité sextique $\Rightarrow$ Algorithmes polynomial, probabilistes

- Test de Miller-Rabin
- Test de Sollovay-Strassen

Tests de primalité probabilistes

Tests de primalité probabilistes

Si n est premier alors :

Ainsi 15 n'est pas premier car :

Tests de primalité probabilistes

Si n est premier alors :

$\forall x \in [2..n-1],\ x \nmid n$ [$\nexists$ de diviseur strict]

Ainsi 15 n'est pas premier car :

$3 \mid 15$ $\sharp = 2$ [$\exists$ un diviseur strict]

Tests de primalité probabilistes

Si n est premier alors :

$\forall x \in [2..n-1],\ x \nmid n$ [$\nexists$ de diviseur strict]

$\forall x \in [2..n-1],\ \text{pgcd}(x,n) = 1$ [$\nexists$ de pgcd non trivial]

Ainsi 15 n'est pas premier car :

$3 \mid 15$ $\sharp = 2$ [$\exists$ un diviseur strict]

$\text{pgcd}(6,15) \neq 1$ $\sharp = 7$ [$\exists$ un pgcd non trivial]

Tests de primalité probabilistes

Si n est premier alors :

$\forall x \in [2..n-1],\ x \nmid n$ [$\nexists$ de diviseur strict]

$\forall x \in [2..n-1],\ \text{pgcd}(x,n) = 1$ [$\nexists$ de pgcd non trivial]

$\forall x \in [2..n-1],\ x^{n-1} \equiv 1 \pmod{n}$ [Petit Fermat]

Ainsi 15 n'est pas premier car :

$3 \mid 15$ $\sharp = 2$ [$\exists$ un diviseur strict]

$\text{pgcd}(6,15) \neq 1$ $\sharp = 7$ [$\exists$ un pgcd non trivial]

$2^{15-1} \equiv 4 \pmod{15}$ $\sharp = 10$ [$\neq$ Petit Fermat]

Tests de primalité probabilistes

Si n est premier alors :

$$\forall x \in [2..n-1],\ x \nmid n \qquad [\nexists \text{ de diviseur strict}]$$

$$\forall x \in [2..n-1],\ \text{pgcd}(x,n) = 1 \qquad [\nexists \text{ de pgcd non trivial}]$$

$$\forall x \in [2..n-1],\ x^{n-1} \equiv 1 \pmod{n} \qquad [\text{Petit Fermat}]$$

$$\forall x \in [2..n-1],\ \begin{array}{l} x^r \equiv 1 \bmod n \text{ ou } \exists i < \alpha, \\ x^{2^i r} = -1 \bmod n \\ n-1 = 2^\alpha r,\ r \text{ impair} \end{array} \qquad [\text{Ordre}]$$

Ainsi 15 n'est pas premier car :

$$3 \mid 15 \qquad \sharp = 2 \qquad [\exists \text{ un diviseur strict}]$$

$$\text{pgcd}(6,15) \neq 1 \qquad \sharp = 7 \qquad [\exists \text{ un pgcd non trivial}]$$

$$2^{15-1} \equiv 4 \pmod{15} \qquad \sharp = 10 \qquad [\neq \text{Petit Fermat}]$$

Tests de primalité de Miller-Rabin

Tests de primalité de Miller-Rabin

Rabin

Si n est composé (i.e. non premier) alors :

$$\frac{1}{n} \times \sharp\{x \in [1..n],\ \text{témoin de non primalité de Miller}\} \geq \frac{3}{4}$$

Tests de primalité de Miller-Rabin

Rabin

Si n est composé (i.e. non premier) alors :

$$\frac{1}{n} \times \sharp \{x \in [1..n], \text{ témoin de non primalité de Miller}\} \geq \frac{3}{4}$$

Il en résulte une test de primalité, probabiliste de complexité cubique : il requiert un nombre d'opérations élémentaires de l'ordre de $O(\log(n)^3)$.

Tests de primalité de Miller-Rabin

Rabin

Si n est composé (i.e. non premier) alors :

$$\frac{1}{n} \times \sharp \{x \in [1..n], \text{ témoin de non primalité de Miller}\} \geq \frac{3}{4}$$

Il en résulte une test de primalité, probabiliste de complexité cubique : il requiert un nombre d'opérations élémentaires de l'ordre de $O(\log(n)^3)$.
Toutes les étapes de création et de fonctionnement d'un protocole RSA sont maintenant effectives... sauf évidemment celles consistant à déterminer les données privées.

Tests de primalité de Miller-Rabin

Rabin

Si n est composé (i.e. non premier) alors :

$$\frac{1}{n} \times \sharp \{x \in [1..n], \text{ témoin de non primalité de Miller}\} \geq \frac{3}{4}$$

Il en résulte une test de primalité, probabiliste de complexité cubique : il requiert un nombre d'opérations élémentaires de l'ordre de $O(\log(n)^3)$.
Toutes les étapes de création et de fonctionnement d'un protocole RSA sont maintenant effectives... sauf évidemment celles consistant à déterminer les données privées.
RSA est bel et bien un protocole de cryptographie à clé publique.