Bribes de cryptographie

L1 cursus prépa.

3 décembre 2014

Le pays des facteurs malhonnêtes

Alice et Bob vivent loin l'une de l'autre. Bob veut envoyer un objet de valeur à Alice mais tous les paquets non cadenassés sont pillés par Ève, le facteur. Alice et Bob peuvent acheter des cadenas inviolables mais seul l'acheteur en possède la clé. Comment faire ?

Le pays des facteurs malhonnêtes

Alice et Bob vivent loin l'une de l'autre. Bob veut envoyer un objet de valeur à Alice mais tous les paquets non cadenassés sont pillés par Ève, le facteur. Alice et Bob peuvent acheter des cadenas inviolables mais seul l'acheteur en possède la clé. Comment faire ?

Réponse :

- Bob cadenasse le paquet et l'envoie à Alice ;
- Alice ajoute un cadenas au paquet et l'envoie à Bob ;
- Bob enlève son cadenas et envoie le paquet à Alice ;
- Alice ouvre le paquet.

Au lieu de cadenas, des fonctions trappes

Une *fonction trappe* est une fonction bijective f qui est facile à calculer mais dont l'inverse f^{-1} est difficile à calculer.

Au lieu de cadenas, des fonctions trappes

Une *fonction trappe* est une fonction bijective f qui est facile à calculer mais dont l'inverse f^{-1} est difficile à calculer.

Exemple : Fixe p premier (public), d entier :

$$f : g \mapsto g^d \quad (p)$$

(facile à calculer).

Au lieu de cadenas, des fonctions trappes

Une *fonction trappe* est une fonction bijective f qui est facile à calculer mais dont l'inverse f^{-1} est difficile à calculer.

Exemple : Fixe p premier (public), d entier secret :

$$f : g \mapsto g^d \quad (p)$$

(facile à calculer).

- Connaissant d, on trouve e tel que $de \equiv 1 \ (p-1)$ (facilement, par Euclide). Alors, par Fermat,

$$f^{-1} : g \mapsto g^e \quad (p)$$

car $\left(g^d\right)^e \equiv g^{de} \equiv g^{1+k(p-1)} \equiv g \times \left(g^{p-1}\right)^k \equiv g \ (p)$.

- Sans connaître d, il semble très difficile de calculer f^{-1}.

(NB : quelques valeurs de d à éviter pour que f soit bijective...)

Variante : partage de secret

Alice et Bob veulent échanger un secret mais leurs communications sont espionnées par Ève.

- Alice et Bob fixent p premier et g « générateur » (publics) ;
- Alice choisit a (secret), calcule $A \equiv g^a \ (p)$ et l'envoie à Bob ;
- Bob choisit b (secret), calcule $B \equiv g^b \ (p)$ et l'envoie à Alice ;
- Alice calcule $B^a = g^{ab} \ (p)$, Bob calcule $A^b \equiv g^{ab} \ (p)$:
  Alice et Bob partagent un secret : $g^{ab} \ (p)$.
  (Alors que A et B peuvent être rendus publics.)

Calculer un produit : facile

Combien de temps ? $\left[(18 \text{ chiffres}) \times (16 \text{ chiffres})\right]$

$$\begin{array}{rr} & 7\,0\,1\,2\,0\,8\,2\,3\,7\,3\,2\,1\,0\,9\,7\,1\,9\,8 \\ \times & 5\,6\,9\,8\,0\,4\,1\,1\,5\,1\,3\,9\,2\,4\,7\,2 \\ \hline \end{array}$$

Calculer un produit : facile

Combien de temps ? $\left[(18 \text{ chiffres}) \times (16 \text{ chiffres})\right]$

$$
\begin{array}{r}
7\,0\,1\,2\,0\,8\,2\,3\,7\,3\,2\,1\,0\,9\,7\,1\,9\,8 \\
\times \quad 5\,6\,9\,8\,0\,4\,1\,1\,5\,1\,3\,9\,2\,4\,7\,2 \\
\hline
1\,4\,0\,2\,4\,1\,6\,4\,7\,4\,6\,4\,2\,1\,9\,4\,3\,9\,6 \\
4\,9\,0\,8\,4\,5\,7\,6\,6\,1\,2\,4\,7\,6\,8\,0\,3\,8\,6 \\
2\,8\,0\,4\,8\,3\,2\,9\,4\,9\,2\,8\,4\,3\,8\,8\,7\,9\,2 \\
1\,4\,0\,2\,4\,1\,6\,4\,7\,4\,6\,4\,2\,1\,9\,4\,3\,9\,6 \\
6\,3\,1\,0\,8\,7\,4\,1\,3\,5\,8\,8\,9\,8\,7\,4\,7\,8\,2 \\
2\,1\,0\,3\,6\,2\,4\,7\,1\,1\,9\,6\,3\,2\,9\,1\,5\,9\,4 \\
7\,0\,1\,2\,0\,8\,2\,3\,7\,3\,2\,1\,0\,9\,7\,1\,9\,8 \\
3\,5\,0\,6\,0\,4\,1\,1\,8\,6\,6\,0\,5\,4\,8\,5\,9\,9\,0 \\
7\,0\,1\,2\,0\,8\,2\,3\,7\,3\,2\,1\,0\,9\,7\,1\,9\,8 \\
7\,0\,1\,2\,0\,8\,2\,3\,7\,3\,2\,1\,0\,9\,7\,1\,9\,8 \\
2\,8\,0\,4\,8\,3\,2\,9\,4\,9\,2\,8\,4\,3\,8\,8\,7\,9\,2 \\
5\,6\,0\,9\,6\,6\,5\,8\,9\,8\,5\,6\,8\,7\,7\,7\,5\,8\,4 \\
6\,3\,1\,0\,8\,7\,4\,1\,3\,5\,8\,8\,9\,8\,7\,4\,7\,8\,2 \\
4\,2\,0\,7\,2\,4\,9\,4\,2\,3\,9\,2\,6\,5\,8\,3\,1\,8\,8 \\
3\,5\,0\,6\,0\,4\,1\,1\,8\,6\,6\,0\,5\,4\,8\,5\,9\,9\,0 \\
\hline
3\,9\,9\,5\,5\,1\,3\,3\,9\,1\,9\,5\,0\,9\,9\,0\,4\,3\,3\,9\,9\,2\,6\,8\,0\,5\,5\,7\,4\,9\,3\,4\,5\,6
\end{array}
$$

$$\begin{array}{rl} & A \\ \times & B \\ \hline & P \end{array} \qquad \begin{array}{l} (a \text{ chiffres}) \\ (1 \text{ chiffre}) \end{array} \Bigg\} \quad \begin{array}{l} a \text{ multiplications} \\ \text{au plus } a \text{ retenues} \end{array}$$

$$\begin{array}{rl} & A \\ \times & B \\ \hline & P_1 \\ & P_2 \\ & \vdots \\ & P_b \\ \hline & N \end{array} \qquad \begin{array}{l} (a \text{ chiffres}) \\ (b \text{ chiffres}) \\ \\ \\ \\ \\ \\ \\ \end{array} \Bigg\} (b \text{ lignes})$$

Bilan : environ ab multiplications, environ autant d'additions.

(On peut faire mieux mais c'est plus compliqué.)

Factoriser : quel temps de calcul ?

On veut factoriser un entier N.
Méthode naïve : essayer tous les entiers entre 2 et N .

Nombre de divisions pour un nombre à n chiffres ?

Factoriser : quel temps de calcul ?

On veut factoriser un entier N.
Méthode naïve : essayer tous les entiers entre 2 et $\sqrt{N}$.

Nombre de divisions pour un nombre à n chiffres ? Environ $10^{n/2}$.

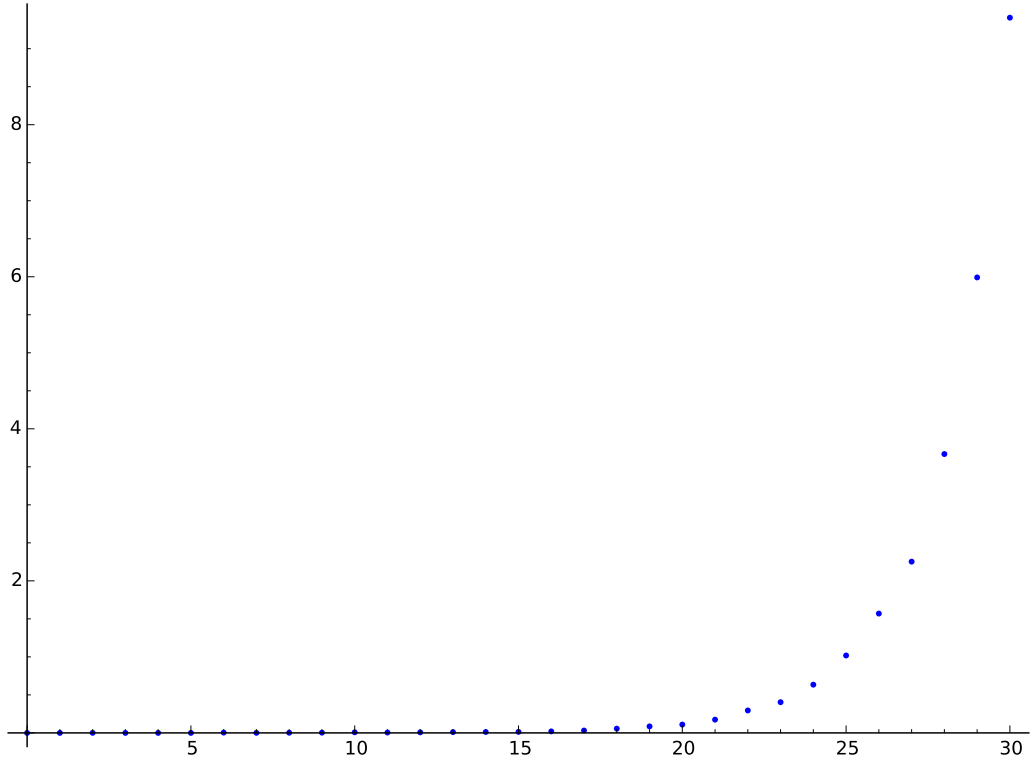
Ex. : si N a $n = 400$ chiffres, il faudra faire 10^{200} divisions.
Un gros ordinateur fait environ 10^{10} opérations par seconde.
Âge de la Terre : environ 5 milliards d'années ou $1,5 \times 10^{17}$ s.
C'est impossible !

On sait faire (un peu) mieux mais c'est difficile. Ex. :

- multiplier deux nombres premiers à 30 chiffres : instantané,
- factoriser ce produit : 10 secondes.

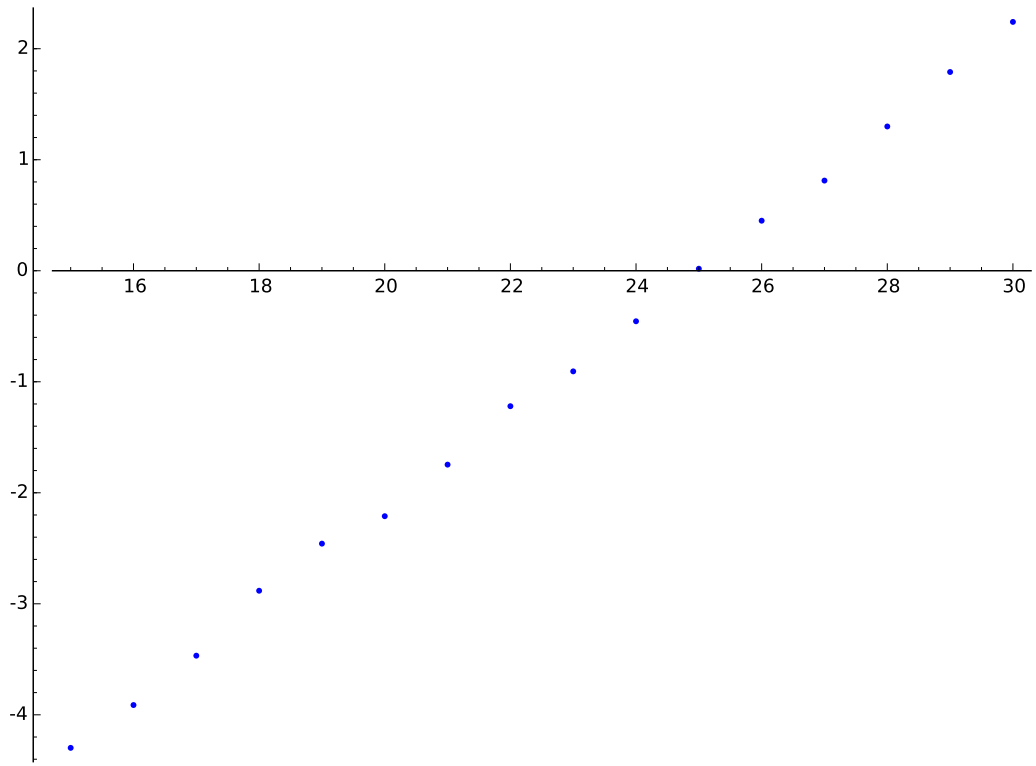
Temps de factorisation

Calculs faits sur un processeur à 2.5 GHz avec un logiciel spécialisé, PARI-GP (via la plateforme Sage).
Temps de calcul pour factoriser deux nombres premiers à d chiffres en fonction de d.



Temps de factorisation

Calculs faits sur un processeur à 2.5 GHz avec un logiciel spécialisé, PARI-GP (via la plateforme Sage).
Logarithme du temps de calcul pour factoriser deux nombres premiers à d chiffres en fonction de d.



Quelques temps de calcul

Temps pour...

- fabriquer un nombre premier à 30 chiffres : environ 0,02 s
- factoriser un nombre à 60 chiffres : environ 10 s

- fabriquer un nombre premier à 50 chiffres : environ 0,06 s
- factoriser un nombre à 100 chiffres : [pas eu la patience...]

- fabriquer un nombre premier à 300 chiffres : environ 20 s
- factoriser un nombre à 600 chiffres : environ infini...

Quelle importance ?

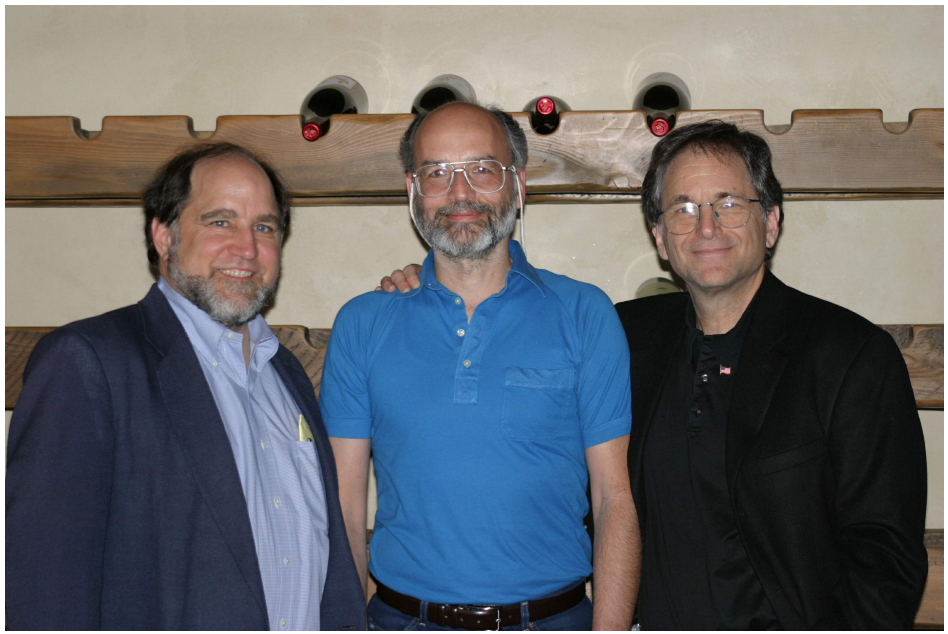
Très grande en pratique !

Raison : méthode de cryptage RSA (Rivest-Shamir-Adleman).

Quelle importance ?

Très grande en pratique !

Raison : méthode de cryptage RSA (Rivest-Shamir-Adleman).



Esquisse du protocole RSA : cryptographie à clé publique

Cryptographie : Bob veut envoyer un message secret S à Alice. Mais Ève, l'espionne, peut l'intercepter. Comment peut faire Bob pour envoyer un message que *seule* Alice puisse comprendre ?

Esquisse du protocole RSA : cryptographie à clé publique

Cryptographie : Bob veut envoyer un message secret S à Alice. Mais Ève, l'espionne, peut l'intercepter. Comment peut faire Bob pour envoyer un message que *seule* Alice puisse comprendre ?

- Alice
  - choisit A et B nombres premiers (*secrets*, environ 200 chiffres)
  - calcule $N = AB$ et le rend public ;
- Alice
  - choisit d (« clé publique »)
  - calcule e tel que $de \equiv (p-1)(q-1)$ (« clé secrète ») ;
- Bob code son message : $M \equiv S^d \ (N)$ et l'envoie à Alice ;
- Alice peut décoder le message : $M^e \equiv S^{de} \equiv S \ (N)$ mais (sans doute) pas Ève si elle ne connaît pas A et B !

Ingrédients : Fermat, exponentiation rapide, lemme chinois (transforme des calculs modulo N en calculs modulo p et q).

Quelle importance ?

Utilisation de la cryptographie (et donc de factorisation) :

- cartes bleues,
- communications militaires,
- internet (commerce, banques, etc.).

Le plus gros employeur de mathématiciens du monde (en 2008) ?

Quelle importance ?

Utilisation de la cryptographie (et donc de factorisation) :

- cartes bleues,
- communications militaires,
- internet (commerce, banques, etc.).

Le plus gros employeur de mathématiciens du monde (en 2008) ?

(D'après James Bamford, journaliste au New York Times.)