Systèmes R.S.A. et El Gamal

Arithmétique et cryptographie

Sommaire

1. Système R.S.A.

1. Système R.S.A.

Cryptographie asymétrique : rappel

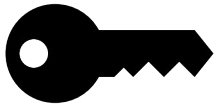
- Un système de chiffrement est dit **asymétrique** si la clé utilisée lors du chiffrement est différente de celle utilisée lors du déchiffrement.

- Un tel système est aussi qualifié de **système de chiffrement à clé publique**.

1. Système R.S.A.

Cryptographie asymétrique : rappel

- Les correspondants ont chacun une clé qu’ils gardent secrète et une clé dite publique qu’ils communiquent à tous.
- Pour envoyer un message, on le chiffre à l’aide de la clé publique du destinataire.
- Celui-ci utilisera sa clé secrète pour le déchiffrer.



1. Système R.S.A.

Système R.S.A. : objectif

- On va présenter ici le premier algorithme de cryptographie asymétrique, développé en 1977 par Rivest, Shamir et Adleman.
- Cet algorithme aura également un côté polygrammique.
- Il reste, sous certaines conditions, le plus sécurisé.

1. Système R.S.A.

Génération des clés du système R.S.A. : principe

- On commence par choisir deux nombres premiers p et q très grands.
- On pose alors $n = pq$ et $m = (p-1)\,(q-1)$.
- On choisit ensuite d très grand tel que d soit premier avec m.
- Enfin, on détermine c, l’inverse multiplicatif modulo m de d.
- La clé publique sera le couple (c,n) et la clé secrète sera l’entier d.

1. Système R.S.A.

Génération des clés du système R.S.A. : exemple

- Soit $p = 47$ et $q = 59$.

- On a donc $n = pq = 47 \times 59 = 2773$ et $m = (p-1)(q-1) = 46 \times 58 = 2668$.

- On choisit alors d premier avec 2668 par exemple $d = 157$.

1. Système R.S.A.

Génération des clés du système R.S.A. : exemple

- On calcule ensuite c l'inverse multiplicatif de 157 modulo 2668 à l'aide des coefficients de Bézout de 157 et 2668

$$157 \times 17 + 2668 \times (-1) = 1$$

- On trouve ainsi $c = 17$.

- Dans cet exemple la clé publique est donc le couple $(17{,}2773)$ et la clé secrète l'entier 157.

1. Système R.S.A.

Convention de représentation des lettres

- Comme pour les algorithmes du chapitre précédent il convient au préalable d'associer à chaque caractère un entier. Voici la convention utilisée en général lors de l'utilisation du système R.S.A.

espace	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

- On confondra une lettre et l’entier la représentant.

1. Système R.S.A.

Prétraitement du message à chiffrer

- On commence par convertir le message à chiffrer en une suite de chiffres selon la convention précédente.

- On découpe cette suite de chiffres en blocs de mêmes longueurs, en ajoutant éventuellement des 0 à la fin.

- Contrainte fondamentale : la valeur numérique de chaque bloc doit être inférieure à n.

1. Système R.S.A.

Formule de chiffrement du R.S.A.

- Soit (c,n) une clé publique.

- Un bloc de chiffres x du message d'origine tel que $x < n$ sera chiffré par le bloc de chiffres y vérifiant

$$y \equiv x^c \, [n]$$

1. Système R.S.A.

Formule de chiffrement du R.S.A. : exemple

- On reprend la clé publique $(c,n) = (17,2773)$.
- Cherchons à chiffrer “its all greek to me“.
- On convertit ce message en une suite de chiffres :

$$092019000112120007180505110020150001305$$

1. Système R.S.A.

Formule de chiffrement du R.S.A. : exemple

- La valeur numérique de chacun des blocs doit être inférieure à $n = 2773$, donc l'on peut faire des blocs de 4 chiffres :

$$0920\ 1900\ 0112\ 1200\ 0718\ 0505\ 1100\ 2015\ 0013\ 0500$$

- À noter que l'on a rajouté deux 0 à la fin pour que le dernier bloc soit lui aussi de 4 chiffres.

1. Système R.S.A.

Formule de chiffrement du R.S.A. : exemple

- Le premier bloc $x = 0920$ est alors chiffré en

$$y \equiv 920^{17} \equiv 948\,[2773]$$

- On procède de même pour les autres blocs et l'on obtient

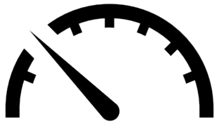
$$0948\ 2342\ 1084\ 1444\ 2263\ 2390\ 0778\ 0774\ 0219\ 1655$$

1. Système R.S.A.

Formule de chiffrement du R.S.A. : remarque

- C'est en particulier ce calcul de puissance qui rend cet algorithme très lent quand il est utilisé avec de grands nombres.

- Une méthode pour calculer une puissance plus rapidement que celle naïve consistant à multiplier un nombre par lui-même autant de fois que son exposant est celle de l'exponentiation rapide.



1. Système R.S.A.

Formule de déchiffrement du R.S.A.

- Soit (c,n) une clé publique et d la clé secrète correspondante.

- Un bloc de chiffres y du message chiffré correspondra au bloc de chiffres x du message d'origine vérifiant

$$x \equiv y^d \, [n]$$

1. Système R.S.A.

Formule de déchiffrement du R.S.A. : démonstration

- Le but est de montrer que si l'on applique la formule de déchiffrement à un y de la forme $y \equiv x^c\,[n]$, alors le résultat est x. Cela revient à vérifier que $x^{cd} \equiv x\,[n]$.

- On va commencer par prouver que $x^{cd} \equiv x\,[p]$.

- Par hypothèse on a $cd \equiv 1\,[m]$, ainsi il existe un entier k tel que $cd = 1 + km$.

- On va alors distinguer deux cas, selon que x soit ou pas divisible par p.

1. Système R.S.A.

Formule de déchiffrement du R.S.A. : démonstration

- Si x n'est pas divisible par p :
  - D'après le petit théorème de Fermat, $x^{p-1} \equiv 1\ [p]$.
  - On a alors $x^{(p-1)(q-1)} \equiv 1\ [p]$, *i.e.* $x^m \equiv 1\ [p]$ et par suite $x^{km} \equiv 1\ [p]$.
  - D'où finalement $x^{cd} \equiv x^{1+km} \equiv xx^{km} \equiv x\ [p]$.

1. Système R.S.A.

Formule de déchiffrement du R.S.A. : démonstration

- Si x est divisible par p :
  - On a bien sûr aussi x^{cd} divisible par p.
  - Ainsi $x^{cd} \equiv 0\,[p]$ et $x \equiv 0\,[p]$ donc $x^{cd} \equiv x\,[p]$.
- Dans les deux cas, x ou non divisible par p, on a bien $x^{cd} \equiv x\,[p]$.
- On montrerait de même que $x^{cd} \equiv x\,[q]$.

1. Système R.S.A.

Formule de déchiffrement du R.S.A. : démonstration

- On a donc prouvé que $p|\left(x^{cd}-x\right)$ et que $q|\left(x^{cd}-x\right)$.
- Il est de plus immédiat que $\mathrm{PGCD}\,(p,q) = 1$ car p et q sont des nombres premiers.
- D'après le corollaire du Théorème de Gauss on a alors $pq|\left(x^{cd}-x\right)$, *i.e.* $n|\left(x^{cd}-x\right)$.
- Ce qui signifie exactement que $x^{cd} \equiv x\,[n]$. Q.E.D.

1. Système R.S.A.

Formule de déchiffrement du R.S.A. : exemple

- Rappelons que la clé publique était $(c,n) = (17,2773)$ et la clé secrète l'entier $d = 157$.

- On cherche à déchiffrer le message

$$0948\ 2342\ 1084\ 1444\ 2263\ 2390\ 0778\ 0774\ 0219\ 1655$$

1. Système R.S.A.

Formule de déchiffrement du R.S.A. : exemple

- Le premier bloc $y = 0948$ est alors déchiffré en

$$x \equiv 948^{157} \equiv 920\,[2773]$$

- Ce bloc converti en lettres donne bien “it“ qui était le début de notre message d’origine.

- On procède alors de même pour les autres blocs pour retrouver “its all greek to me“.

1. Système R.S.A.

Système R.S.A. : décryptement

- La sécurité du R.S.A. repose sur l'incapacité à l'heure actuelle de reconstituer en un temps raisonnable la clé secrète d connaissant la clé publique (c,n).

- Cette opération nécessite en effet de factoriser n en $n = pq$.

- Ceci est possible mais les délais de calculs sont énormes dès que n est assez grand.

1. Système R.S.A.

Système R.S.A. : décryptement

- On arrive pour l'instant à factoriser des nombres de 230 chiffres (clés de 768 bits).

- Mais l'on préconise pour des messages très sensibles d'utiliser le R.S.A. avec des nombres n de plus de 600 chiffres (clé de 2048 bits), dont on estime que l'on saura les factoriser en 2079.

1. Système R.S.A.

Système R.S.A. : décryptement

- D'autres attaques sont possibles en cas de mauvaise utilisation du R.S.A.
- En particulier si l'on intercepte le même message envoyé à des destinataires différents.
- Une subtile utilisation du théorème des restes chinois permet alors de reconstituer le message d'origine.
- Cette attaque dite de Hastad peut cependant être déjouée en introduisant des caractères arbitraires différents pour chaque destinataire.

1. Système R.S.A.

2. Système El Gamal.

2. Système El Gamal.

Système El Gamal : objectif

- Le but principal est le même que pour le R.S.A., à savoir implémenter un système de chiffrement à clé publique.
- Il sera lui aussi à caractère polygrammique.
- On ne présentera qu’une version simple de ce système, basée sur l'unique utilisation des nombres entiers. Il en existe une version plus générale, reposant sur la notion de groupe cyclique.

2. Système El Gamal.

Génération des clés du système El Gamal : principe

- On commence par choisir un nombre premier p.
- On choisit ensuite deux entiers a et m tels que $0 \leq a \leq p-2$ et $0 \leq m \leq p-1$.
- On pose alors $n \equiv m^a \, [p]$.
- La clé publique sera le triplet (p,m,n) et la clé secrète l'entier a.

2. Système El Gamal.

Génération des clés du système El Gamal : exemple

- Soit $p = 661$.
- Choisissons $a = 7$ et $m = 23$.
- On a alors $n \equiv m^a \equiv 23^7 \equiv 566\,[661]$.
- Dans cet exemple la clé publique est donc le triplet $(661{,}23{,}566)$ et la clé secrète l'entier 7.

2. Système El Gamal.

Prétraitement du message à chiffrer

- On commence par convertir le message à chiffrer en une suite de chiffres selon la même convention que pour le R.S.A.

- On découpe cette suite de chiffres en blocs de mêmes longueurs, en ajoutant éventuellement des 0 à la fin.

- Contrainte fondamentale : la valeur numérique de chaque bloc doit être inférieure à p.

2. Système El Gamal.

Formule du chiffrement El Gamal

- Soit (p,m,n) une clé publique.
- On commence par choisir un entier k aléatoirement tel que $0 \leq k \leq p-1$.
- Un bloc de chiffres x du message d'origine tel que $x < p$ sera chiffré par le couple de blocs de chiffres (y_1,y_2) vérifiant

$$y_1 \equiv m^k\,[p] \quad \text{et} \quad y_2 \equiv xn^k\,[p]$$

2. Système El Gamal.

Formule du chiffrement El Gamal : exemple

- On reprend la clé publique $(p, m, n) = (661, 23, 566)$.
- Cherchons à chiffrer “supinfo“.
- On convertit ce message en une suite de chiffres :

$$19211609140615$$

2. Système El Gamal.

Formule du chiffrement El Gamal : exemple

- La valeur numérique de chacun des blocs doit être inférieure à $p\ = 661$, donc l'on peut faire des blocs de 3 chiffres :

192 116 091 460 150

- À noter que l'on a rajouté un 0 à la fin pour que le dernier bloc soit lui aussi de 3 chiffres.

2. Système El Gamal.

Formule du chiffrement El Gamal : exemple

- On choisit aléatoirement l'entier $k = 13$.
- Le premier bloc $x = 192$ est alors chiffré en

$$y_1 \equiv 23^{13} \equiv 105\,[661] \quad \text{et} \quad y_2 \equiv 192 \times 566^{13} \equiv 237\,[661]$$

- On procède de même pour les autres blocs et l'on obtient

$$(105{,}237),\ (105{,}515),\ (105{,}102),\ (105{,}150),\ (105{,}495)$$

2. Système El Gamal.

Formule du déchiffrement El Gamal

- Soit (p,m,n) une clé publique et a la clé secrète correspondante.

- Un couple de bloc de chiffres (y_1,y_2) du message chiffré correspondra au bloc de chiffres x du message d'origine vérifiant

$$x \equiv {y_1}^{p-1-a} y_2 \, [p]$$

2. Système El Gamal.

Formule du déchiffrement El Gamal : démonstration

- Le but est de montrer que si l'on applique la formule de déchiffrement à un couple (y_1,y_2) de la forme

$$y_1 \equiv m^k\,[p] \quad \text{et} \quad y_2 \equiv xn^k\,[p]$$

alors le résultat est x.

- Par construction de la clé on a également $n \equiv m^a\,[p]$.

2. Système El Gamal.

Formule du déchiffrement El Gamal : démonstration

- Si l'on remplace y_1, y_2 et n dans la formule de déchiffrement par les expressions précédentes, on obtient

$$y_1{}^{p-1-a} y_2 \equiv \left(m^k\right)^{p-1-a} x\,(m^a)^k \equiv m^{k(p-1-a)} x m^{ak} \equiv m^{k(p-1)} x\,[p]$$

- Or d’après le petit théorème de Fermat $m^{p-1} \equiv 1\,[p]$. Donc $m^{k(p-1)} \equiv 1\,[p]$.

- Par suite $m^{k(p-1)} x \equiv x\,[p]$. Q.E.D.

2. Système El Gamal.

Formule du déchiffrement El Gamal : exemple

- Rappelons que la clé publique était le triplet $(p,m,n) = (661,23,566)$ et la clé secrète l'entier $a = 7$.

- On cherche à déchiffrer le message

$$(105,237),\ (105,515),\ (105,102),\ (105,150),\ (105,495)$$

2. Système El Gamal.

Formule du déchiffrement El Gamal : exemple

- Le premier bloc couple de blocs $(y_1,y_2) = (105,237)$ est alors déchiffré en

$$x \equiv 105^{661-1-7} \times 237 \equiv 192\,[661]$$

- Ce qui était le début de notre message d’origine.

- On procède alors de même pour les autres blocs pour retrouver “supinfo“.

2. Système El Gamal.

Système El Gamal : décryptement

- Comme pour le R.S.A., la sécurité du système El Gamal repose sur la difficulté de calculer la clé secrète a alors que l'on connait la clé publique (p,m,n).

- Cette opération revient en effet à retrouver la valeur de a à partir de celle de $n \equiv m^a\,[p]$.

- Ce problème, connu sous le nom de calcul du logarithme discret, est certes resolvable mais en un temps relativement long.

- À l'heure actuelle, il n'existe par exemple pas d'algorithme à complexité polynomiale effectuant cette tâche.

2. Système El Gamal.