Cryptographie à clé publique : La méthode RSA

Malika More
(malika.more@iut.u-clermont1.fr)
Jean Mailfert - Gisèle Provost

1A - IUT Info - Clermont 1

Arithmétique et Cryptographie

Année 2011-2012

Important

- Les transparents du cours et d'autres documents et informations sont disponibles sur la page du cours sur l'ENT
- Il est très fortement recommandé d'apporter une calculatrice en cours et en TD d'arithmétique

Plan du cours

1. Factorisation de grands nombres
2. La méthode RSA
3. Cryptographie avec la méthode RSA
4. Travail personnel

Introduction

- Comme la méthode du sac-à-dos, la méthode RSA est un cryptosystème à clé publique.
- Elle a été inventée en 1978 par Ronald Rivest, Adi Shamir et Leonard Adleman (R.L. Rivest, A. Shamir, and L. Adleman. **A Method for Obtaining Digital Signatures and Public-Key Cryptosystems**, *Communications of the Association for Computing Machinery*, 21(2) :120-126, 1978).
- Le nom RSA est composé des initiales des noms de famille des inventeurs : **R**(ivest)**S**(hamir)**A**(dleman).

1. Factorisation de grands nombres
2. La méthode RSA
3. Cryptographie avec la méthode RSA
4. Travail personnel

Un problème difficile

- Comme la méthode du sac-à-dos, la méthode RSA est basée sur un problème mathématique difficile à résoudre.
- Nous avons vu dans le chapitre précédent que dans le cas de la méthode du sac-à-dos, le problème difficile était le problème du sac-à-dos.
- Dans le cas de la méthode RSA, le problème difficile sur lequel repose la sécurité du système est celui de la **factorisation**.

La factorisation

- Étant donné un entier n, il s'agit simplement de trouver un diviseur de n.
- On sait qu'il suffit de tester tous les nombres premiers jusqu'à $\sqrt{n}$.
- Ce n'est pas très difficile en théorie, mais en pratique le problème est surtout de disposer de suffisamment de temps.

Une question de temps

- Dans cette feuille, on se limitera à des facteurs premiers inférieurs à 1000.
- Dans la vraie vie, on utilise des nombres n de 300 chiffres environ en base dix.
- Les meilleurs algorithmes de factorisation connus, tournant sur les meilleurs ordinateurs actuels, mettraient plusieurs années à factoriser un produit de deux nombres premiers inconnus de 150 chiffres chacun.
- Par contre, si on dispose de deux nombres, même de 150 chiffres chacun, il est facile de calculer leur produit.

Liste des 168 nombres premiers inférieurs à 1000

2	3	5	7	11	13	17	19	23	29	31	37	41	43	47
53	59	61	67	71	73	79	83	89	97	101	103	107	109	113
127	131	137	139	149	151	157	163	167	173	179	181	191	193	197
199	211	223	227	229	233	239	241	251	257	263	269	271	277	281
283	293	307	311	313	317	331	337	347	349	353	359	367	373	379
383	389	397	401	409	419	421	431	433	439	443	449	457	461	463
467	479	487	491	499	503	509	521	523	541	547	557	563	569	571
577	587	593	599	601	607	613	617	619	631	641	643	647	653	659
661	673	677	683	691	701	709	719	727	733	739	743	751	757	761
769	773	787	797	809	811	821	823	827	829	839	853	857	859	863
877	881	883	887	907	911	919	929	937	941	947	953	967	971	977
983	991	997												

À vous de jouer

Factoriser les nombres suivants : 35 ; 1247 ; 3811 ; 254503.

1. Factorisation de grands nombres
2. La méthode RSA
3. Cryptographie avec la méthode RSA
4. Travail personnel

Encore un peu d'arithmétique

- Les mathématiques nécessaires pour comprendre la méthode RSA sont un peu plus compliquées que dans le cas de la méthode du sac-à-dos.
- Par contre, l'utilisation n'est pas plus difficile, et même par certains côtés plus simple, puisqu'il n'y a plus besoin de passer par des messages binaires.
- Pour commencer, on a besoin de deux propriétés sur le calcul modulaire.

Propriété 1

Pour tous entiers naturels a, b, c, d,

si c et d sont premiers entre eux, et si $\begin{cases} a \equiv b \mod c \\ a \equiv b \mod d \end{cases}$,

alors on a

$$a \equiv b \mod cd$$

Propriété 1

Pour tous entiers naturels a, b, c, d,

si c et d sont premiers entre eux, et si $\begin{cases} a \equiv b \mod c \\ a \equiv b \mod d \end{cases}$,

alors on a

$$a \equiv b \mod cd$$

Démonstration.

- La relation $a \equiv b \mod c$ se réécrit en $a - b \equiv 0 \mod c$.
- Autrement dit, c divise $a - b$
- De même, on montre que d divise $a - b$
- **Comme c et d sont premiers entre eux**, on en déduit que $c \times d$ divise $a - b$
- On peut aussi écrire $a - b \equiv 0 \mod cd$ ou $a \equiv b \mod cd$.
- C'est bien ce qu'on voulait.

Illustration

- Prenons $c = 10$ et $d = 21$, qui sont premiers entre eux.
- Prenons $a = 28 = 10 \times 2 + 8 = 21 \times 1 + 7$
- Et prenons $b = 238 = 10 \times 23 + 8 = 21 \times 11 + 7$
- Autrement dit, on a $\begin{cases} 28 \equiv 238 \equiv 8 \mod 10 \\ 28 \equiv 238 \equiv 7 \mod 21 \end{cases}$
- On a $238 = 210 \times 1 + 28$, c'est-à-dire qu'on a bien :

$$238 \equiv 28 \mod 10 \times 21$$

Contre-illustration

- Prenons $c = 30$ et $d = 35$, qui ne sont pas premiers entre eux.
- Prenons $a = 38 = 30 \times 1 + 8 = 35 \times 1 + 3$
- Et prenons $b = 248 = 30 \times 8 + 8 = 35 \times 7 + 3$
- Autrement dit, on a $\begin{cases} 38 \equiv 248 \equiv 8 \mod 30 \\ 38 \equiv 248 \equiv 3 \mod 35 \end{cases}$
- Par contre $30 \times 35 = 1050$ et clairement

$$38 \not\equiv 248 \mod 1050$$

Propriété 2

Pour tous nombres premiers différents p, q *et pour tous entiers* e, d, m, *si* $ed \equiv 1 \mod (p-1)\times(q-1)$ *alors on a*

$$m^{ed} \equiv m \mod pq$$

Démonstration.

Propriété 2

Pour tous nombres premiers différents p, q *et pour tous entiers* e, d, m, *si* $ed \equiv 1 \mod (p-1) \times (q-1)$ *alors on a*

$$m^{ed} \equiv m \mod pq$$

Démonstration.

- Comme p et q sont premiers et différents, ils sont premiers entre eux.
- Donc il suffit de montrer que $m^{ed} \equiv m \mod p$ et $m^{ed} \equiv m \mod q$ séparément, d'après la Propriété 1.
- On commence par montrer que $m^{ed} \equiv m \mod p$

Propriété 2

Pour tous nombres premiers différents p, q et pour tous entiers e, d, m, si $ed \equiv 1 \mod (p-1) \times (q-1)$ alors on a

$$m^{ed} \equiv m \mod pq$$

Démonstration.

- On a $ed \equiv 1 \mod (p-1) \times (q-1)$, ce qui signifie que $ed = k(p-1) \times (q-1) + 1$ pour un certain $k \in \mathbb{N}$.
- Il y a deux cas : ou bien m et p sont premiers entre eux, ou bien ils ne le sont pas.

Propriété 2

Pour tous nombres premiers différents p, q *et pour tous entiers* e, d, m, *si* $ed \equiv 1 \mod (p-1)\times(q-1)$ *alors on a*

$$m^{ed} \equiv m \mod pq$$

Démonstration.

- Si m et p sont premiers entre eux, on peut uiliser le théorème de Fermat : on a $m^{(p-1)} \equiv 1 \mod p$. Or $m^{ed} = m^{k(p-1)\times(q-1)+1} = \left(m^{(p-1)}\right)^{k(q-1)} \times m$
- Autrement dit $m^{ed} \equiv (1)^{k(q-1)} \times m \equiv m \mod p$
- C'est bien ce qu'on voulait

Propriété 2

Pour tous nombres premiers différents p, q et pour tous entiers e, d, m, si $ed \equiv 1 \mod (p-1) \times (q-1)$ alors on a

$$m^{ed} \equiv m \mod pq$$

Démonstration.

- Si m et p ne sont pas premiers entre eux, cela signifie que p divise m. Par conséquent, $m \equiv 0 \mod p$ et bien sûr aussi $m^{ed} \equiv 0 \mod p$. On a bien aussi $m^{ed} \equiv m \mod p$.
- Ensuite, on refait le même raisonnement en remplaçant partout p par q, et on obtient que $m^{ed} \equiv m \mod q$
- Finalement, on a bien $m^{ed} \equiv m \mod pq$.

□

Et c'est parti !

- **Créer un chiffre RSA :**
  - Choisir deux (grands) nombres premiers différents p et q qui devront rester secrets.

Exemple

On choisit $p = 11$ et $q = 17$.

  - Calculer le *module* $N = p \times q$. Ce module sera public, mais comme le problème de la factorisation est difficile, on ne pourra pas se servir de N pour retrouver p et q.

Exemple

On calcule $N = 11 \times 17 = 187$.

- **Créer un chiffre RSA (suite) :**
  - Calculer $\varphi = (p-1) \times (q-1)$. Ce nombre φ devra rester secret. Comme p et q sont secrets, on ne pourra pas s'en servir pour calculer φ.

Exemple

On calcule $\varphi = 10 \times 16 = 160$.

  - Choisir un (grand) *compliqueur* E tel que $E < \varphi$ et $pgcd(\varphi, E) = 1$. Ce compliqueur sera public. Comme $pgcd(\varphi, E) = 1$, le compliqueur E est inversible modulo φ.

Exemple

On choisit $E = 13$. On vérifie que $pgcd(13, 160) = 1$.

- **Créer un chiffre RSA (suite) :**
  - Calculer le *faciliteur* $D = E^{-1} \mod \varphi$. Le faciliteur devra rester secret. Le compliqueur E est public, mais comme φ est secret, on n'aura aucun moyen de calculer l'inverse de E modulo φ. On note qu'on a $ED \equiv 1 \mod \varphi$, puisque le faciliteur D est l'inverse du compliqueur E modulo φ.

Exemple

On calcule $D \equiv (13)^{-1} \mod 160 \equiv 37 \mod 160$.

- **Créer un chiffre RSA (fin) :**
  - La *clé publique* est constituée du compliqueur E et du module N.

Exemple

Clé publique : $E = 13$ et $N = 187$.

  - La *clé privée* est constituée du faciliteur D.

Exemple

Clé privée : $D = 37$.

- **Chiffrer un message M :**
  - Vérifier que le message M est inférieur au module N

Exemple

On veut envoyer $M = 4$. On vérifie que $4 < 187$.

  - Calculer le cryptogramme C à l'aide du compliqueur : $C \equiv M^E \mod N$. Les nombres C, E et N sont publics, mais il n'y a aucun moyen de retrouver le message d'origine M, sauf à essayer tous les messages possibles pour voir quel est celui qui marche. Et ça prendrait trop de temps.

Exemple

On calcule $C \equiv 4^{13} \mod 187 \equiv 174 \mod 187$.

- **Déchiffrer un cryptogramme C :**
  - Calculer $M' \equiv C^D \mod N$. C'est ici qu'intervient la Propriété 2 : on a $M' \equiv C^D \mod N \equiv (M^E)^D \mod N \equiv M^{ED} \mod N$ avec $ED \equiv 1 \mod \varphi(N)$ et $N = p \times q$, produit de deux nombres premiers différents. Donc on peut appliquer la Propriété 2, et on en déduit que $M' \equiv M \mod N$. Comme en plus on a pris soin au départ que le message M satisfasse $M < N$, ce $\equiv$ est en fait un $=$, c.-à-d. $M' = M$, autrement dit cette méthode permet bien de récupérer le message d'origine.

Exemple

On calcule $M' \equiv 174^{37} \mod 187 \equiv 4 \mod 187$.

Résumé

- Créer un chiffre RSA :
  - Choisir deux nombres premiers différents p et q.
  - Calculer le *module* $N = p \times q$.
  - Calculer $\varphi = (p-1) \times (q-1)$.
  - Choisir un *compliqueur* E tel que $E < \varphi$ et $pgcd(\varphi, E) = 1$.
  - Calculer le *faciliteur* $D = E^{-1} \mod \varphi$.
  - La *clé publique* est constituée du compliqueur E et du module N.
  - La *clé privée* est constituée du faciliteur D.
- Chiffrer un message M :
  - Vérifier que le message M est inférieur au module N
  - Calculer le cryptogramme $C = M^E \mod N$.
- Déchiffrer un cryptogramme C :
  - Calculer $M' = C^D \mod N$.

À vous de jouer !

La clé publique de Bob est $N = 247$ et $E = 11$, et sa clé privée est $D = 59$.

1. Aidez Alice à chiffrer le message clair $M = 100$ pour l'envoyer à Bob.
2. Le cryptogramme $C = 52$ est reçu par Bob. Aidez-le à le déchiffrer.

À vous de jouer !

1. Pour fabriquer son chiffre RSA, Bob a choisi les deux nombres premiers $p = 13$ et $q = 23$. Calculer le module N et le nombre φ.
2. Bob doit maintenant choisir son compliqueur E. Le nombre 41 constitue-t-il un compliqueur acceptable ? Pourquoi ? Le nombre 72 constitue-t-il un compliqueur acceptable ? Pourquoi ?
3. Réflexion faite, Bob a choisi le compliqueur $E = 83$ (on ne vous demande pas de vérifier qu'il est acceptable). Calculer le faciliteur correspondant D.
4. Bob va maintenant publier la partie publique de son chiffre RSA. Indiquez de quoi est constituée cette partie publique.

Exercice 1

Alice a publié la partie publique de son chiffre RSA : $E_A = 179$ et $N_A = 629$. La partie privée de son chiffre est $D_A = 251$. Bob a publié la partie publique de son chiffre RSA : $E_B = 601$ et $N_B = 851$. La partie privée de son chiffre est $D_B = 481$.
Alice veut envoyer un message (codé numériquement par un seul nombre $M = 342$) à Bob.

1. Quel est le calcul que doit effectuer Alice pour chiffrer son message ? Vous noterez C le message chiffré.
2. Quel est le calcul que doit effectuer Bob pour déchiffrer C ? Vous noterez M' le message déchiffré.

Exercice 2

Alice a publié la clef publique de son chiffre RSA : $N = 391$ et $E = 151$, et elle a conservé en lieu sûr sa clef privée $D = 7$.

1. Bob lui transmet un message sous la forme du nombre : $C = 17$. Quelle opération Alice va-t-elle effectuer pour déchiffrer ce message ? Quel nombre va-t-elle obtenir ?
2. Retrouvez les deux nombres premiers p et q (le nombre N étant petit, c'est faisable). En déduire $\varphi(N)$.
3. Quelle relation existe-t-il entre E et D ? Vérifiez cette relation sur les nombres donnés.

Exercice 3

1. On considère un chiffre RSA constitué du module $N = 221$, du compliqueur $E = 11$ et du faciliteur $D = 35$. On ne demande pas de vérifier que ces valeurs sont acceptables.
    1. Chiffrer le message $M = 112$.
    2. Déchiffrer le cryptogramme $C = 78$.
2. Pour fabriquer un chiffre RSA, on a choisi $p = 53$ et $q = 71$.
    1. Calculer le module N et le nombre $\varphi(N)$.
    2. On choisit le compliqueur $E = 307$. Vérifier qu'il est acceptable et calculer le faciliteur correspondant D.
    3. Indiquer quels sont les éléments qui constituent la clé publique et quels sont les éléments qui constituent la clé privée de ce chiffre RSA.
    4. Que faut-il faire des éléments restants ? Pourquoi ?

Exercice 4

Travail en binôme

1. Créez chacun un chiffre RSA **personnel**. Pour que les calculs ne soient pas trop pénibles, je vous conseille de choisir des nombres p et q inférieurs à 50.
2. Communiquez votre clé publique à votre binôme.
3. Procurez-vous la clé publique de votre binôme.
4. Choisissez un message et chiffrez-le pour l'adresser à votre binôme.
5. Récupérez le cryptogramme que vous a adressé votre binôme et déchiffrez-le.
6. Vérifiez avec votre binôme que vous avez tous les deux réussi l'exercice.

1. Factorisation de grands nombres
2. La méthode RSA
3. Cryptographie avec la méthode RSA
4. Travail personnel

Comme d'habitude

- Pour envoyer de vrais messages secrets avec un chiffre RSA, il faut commencer par convenir de la façon de trancrire les messages alphabetiques en messages numériques.
- On utilise la correspondance habituelle entre les lettres de l'alphabet $\{A, B, C, \ldots, Z\}$ et les nombres $\{0, 1, 2, \ldots, 25\}$.

A	B	C	D	E	F	G	H	I	J	K	L	M
00	01	02	03	04	05	06	07	08	09	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Une règle de bon sens

- Si on se contente de chiffrer séparément chaque lettre du message, le cryptogramme obtenu pourra être attaqué par l'analyse des fréquences, puisque chaque lettre sera toujours chiffrée par le même nombre.
- De même si on prend des blocs de deux lettres, etc.
- Une méthode possible pour éviter ce problème (et qui sera réutilisée en TP en période 4) consiste à prendre des blocs de chiffres qui ne correspondent pas à un nombre entier de lettres, comme expliqué ci-dessous.

Exemple

On utilise le chiffre RSA suivant :

- La *clé publique* est constituée du compliqueur $E = 257$ et du module $N = 1073$.
- La *clé privée* est constituée du faciliteur $D = 353$.
- Les messages doivent toujours être inférieurs au module $N = 1073$.
- Pour assurer cette condition, on peut par exemple convenir que les messages auront seulement 3 chiffres, soit moins de chiffres que le module qui en a 4.
- On note de plus qu'un bloc de 3 chiffres ne correspond pas à un nombre entier de lettres.

Exemple

- On chiffre le message : *RSA*.
  - Numériquement, *RSA* correspond à 17; 18; 00.
  - On concatène les nombres obtenus : 171800.
  - On découpe en paquets de 3 chiffres : 171; 800.
  - On chiffre chaque paquet séparément :
    - $171^{257} \equiv 859 \mod 1073$
    - $800^{257} \equiv 452 \mod 1073$
  - Le cryptogramme est : 859; 452

Exemple

- On reçoit le cryptogramme : $549; 097$
  - On déchiffre chaque paquet séparément :
    - $549^{353} \equiv 142 \mod 1073$
    - $97^{353} \equiv 8 \mod 1073$
  - Le message déchiffré est : $142; 008$
  - On colle les blocs des trois chiffres obtenus : 142008
  - On découpe en blocs de deux chiffres : $14; 20; 08$
  - Le message est : *OUI*.

Exercice 5

En utilisant le même chiffre RSA que dans l'exemple ci-dessus, chiffrer le message : *SAC*.

Exercice 6

En utilisant le même chiffre RSA que dans l'exemple ci-dessus, déchiffrer le cryptogramme : $553; 813$.

Exercice 7

En utilisant le même chiffre RSA que dans l'exemple ci-dessus, chiffrer le message : *METHODE*.

Exercice 8

En utilisant le même chiffre RSA que dans l'exemple ci-dessus, déchiffrer le cryptogramme : $263; 115; 613; 10$.

Exercice 9

La clé publique de Bob est $N = 203$ et $E = 89$, et sa clé privée est $D = 17$.

1. Aidez Alice à chiffrer le message clair $M = 98$ pour l'envoyer à Bob.
2. Le cryptogramme $C = 142$ est reçu par Bob. Aidez-le à le déchiffrer.

Exercice 10

Alice a publié la partie publique de son chiffre RSA : $E_A = 127$ et $N_A = 403$. La partie privée de son chiffre est $D_A = 343$. Bob a publié la partie publique de son chiffre RSA : $E_B = 305$ et $N_B = 989$. La partie privée de son chiffre est $D_B = 821$.
Alice veut envoyer un message (codé numériquement par un seul nombre $M = 357$) à Bob.

1. Quel est le calcul que doit effectuer Alice pour chiffrer son message ? Vous noterez C le message chiffré.
2. Quel est le calcul que doit effectuer Bob pour déchiffrer C ? Vous noterez M' le message déchiffré.

Exercice 11

1. Pour fabriquer son code RSA, Bob a choisi les deux nombres premiers $p = 37$ et $q = 41$. Calculer le module N et le nombre φ.
2. Bob doit maintenant choisir son compliqueur E. Le nombre 305 constitue-t-il un compliqueur acceptable ? Pourquoi ? Le nombre 59 constitue-t-il un compliqueur acceptable ? Pourquoi ?
3. Réflexion faite, Bob a choisi le compliqueur $E = 73$ (on ne vous demande pas de vérifier qu'il est acceptable). Calculer le faciliteur correspondant D.
4. Bob va maintenant publier la partie publique de son code RSA. Indiquez de quoi est constituée cette partie publique.

Exercice 12

Pour fabriquer un chiffre RSA, on a choisi $p = 29$ et $q = 11$.

1. Calculer le module N et le nombre $\varphi(N)$.
2. On choisit le compliqueur $E = 151$. Vérifier qu'il est acceptable et calculer le faciliteur correspondant D.
3. Indiquer quels sont les éléments qui constituent la clé publique et quels sont les éléments qui constituent la clé privée de ce chiffre RSA.
4. Que faut-il faire des éléments restants ? Pourquoi ?

Exercice 13

Alice a publié la partie publique de son code RSA : e_A et n_A. La partie privée de son code est d_A.
Bob a publié la partie publique de son code RSA : e_B et n_B. La partie privée de son code est d_B.
Bob veut envoyer un message (codé numériquement par un seul nombre M) à Alice.

1. Quel est le calcul que doit effectuer Bob pour chiffrer son message ? Vous noterez C le message chiffré.
2. Quel est le calcul que doit effectuer Alice pour déchiffrer C ? Vous noterez D le message déchiffré.

Exercice 14

On considère un chiffre RSA dont la clé publique est $N = 4189$ et $E = 581$, et la clé privée est $D = 1289$. Déchiffrer le cryptogramme : $3286; 3540; 2244; 730; 342$.

Exercice 15

En utilisant le même chiffre RSA que dans l'exercice ci-dessus, chiffrer le message : *IUTINFO*.

FIN