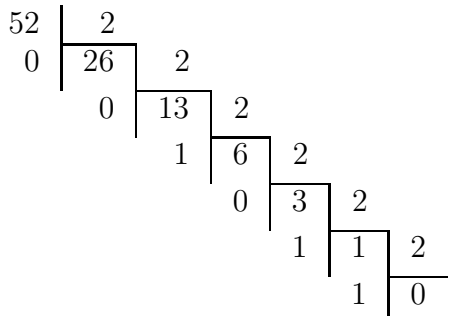
7 Cryptographie (RSA)

Exponentiation modulaire

On verra que le système de cryptage RSA nécessite d'effectuer une exponentiation modulaire, c'est-à-dire de calculer $a^n \mod m$, lorsque m et n sont très grands. Heureusement, il existe un algorithme, appelé l'**exponentiation binaire**, qui réduit considérablement le nombre des opérations.

Illustrons-le en calculant $15^{52} \mod 23$.

On commence par écrire 52 en base 2 comme on l'a fait au chapitre 1 :



On a donc trouvé $52 = \overline{110100} = 2^5 + 2^4 + 2^2$.

Par conséquent $15^{52} = 15^{2^5+2^4+2^2} = 15^{2^5} \cdot 15^{2^4} \cdot 15^{2^2}$.

Il reste encore à déterminer $15^{2^n} \mod 23$ pour $0 \leqslant n \leqslant 5$. Ces valeurs se calculent facilement si l'on remarque que $15^{2^{n+1}} = 15^{2^n \cdot 2} = \left(15^{2^n}\right)^2$: les valeurs successives de 15^{2^n} s'obtiennent en calculant le carré de la précédente :

n	$15^{2^n} \mod 23$
0	15
1	$15^2 \equiv 225 \equiv 18$
2	$18^2 \equiv 324 \equiv 2$
3	$2^2 \equiv 4$
4	$4^2 \equiv 16$
5	$16^2 \equiv 256 \equiv 3$

Finalement, $15^{52} \equiv 15^{2^5} \cdot 15^{2^4} \cdot 15^{2^2} \equiv 3 \cdot 16 \cdot 2 \equiv 96 \equiv 4 \mod 23$.

On peut aussi synthétiser cette démarche sous la forme d'un seul tableau :

x	reste r	n	$15^{2^n} \mod 23$	contribution (si $r = 1$)
52	0	0	15	
26	0	1	$15^2 \equiv 18$	
13	1	2	$18^2 \equiv 2$	2
6	0	3	$2^2 \equiv 4$	
3	1	4	$4^2 \equiv 16$	16
1	1	5	$16^2 \equiv 3$	3

7.1 Calculer :

1) $3^{100} \mod 19$ 2) $12^{364} \mod 34$ 3) $5^{51} \mod 97$ 4) $9^{71} \mod 113$

La cryptographie à clé privée

Les algorithmes de chiffrement utilisés jusqu'à la veille des années 1970, aussi sophistiquées que soient leur méthode de codage, présentent deux inconvénients majeurs : la transmission des clés et l'authentification de l'expéditeur.

Les méthodes traditionnelles de cryptage sont dites **symétriques** ou encore à **clé privée**, parce qu'elles se fondent sur une même clé pour chiffrer et déchiffrer un message. Le problème de cette technique est que la clé, qui doit rester totalement confidentielle, doit être transmise au correspondant de façon sûre. Toute interception, quelle que soit la sécurité du codage, détruit la confidentialité du message. Dans son ouvrage *Histoire des codes secrets*, Simon Singh illustre bien le problème :

> Dans les années 70, les banques essayèrent de faire distribuer les clés par des coursiers spécialement sélectionnés, qui comptaient parmi les employés les plus sûrs de l'entreprise. Ces messages devaient courir le monde munis de cartables cadenassés, et remettre en mains propres les clés aux destinataires des messages de la banque la semaine suivante. Plus les contacts se multipliaient, plus les réseaux s'étendaient, et tant de clés durent être distribuées que la logistique nécessaire, avec ses frais prohibitifs, devint un véritable cauchemar.

L'autre problème est qu'il est impossible de savoir si l'expéditeur d'un message est bien celui que l'on croit. Un intrus, s'étant emparé de la clé, pourrait très bien fabriquer de faux messages, ou changer subrepticement une partie d'un message intercepté. En l'absence d'une **signature** de l'expéditeur, ces falsifications demeurent indétectables.

La cryptographie à clé publique

Le problème de la transmission des clés a été résolu grâce à la cryptographie à clé publique. Pour illustrer son fonctionnement, imaginons qu'Alice et Bob vivent dans un pays à ce point corrompu que le système postal n'offre plus aucune sécurité : toutes les lettres et tous les paquets sont susceptibles d'être ouverts par les employés de la poste. Alice doit faire parvenir à Bob un message très personnel, mais elle n'a ni le temps ni les moyens de le lui transmettre personnellement. Elle ne peut l'envoyer que par la poste. Existe-t-il un moyen de le faire, en étant sûr que Bob reçoive le message sans qu'il ait été lu par un tiers ?

La solution de cette énigme a été trouvée en 1976 par Whitfield Diffie et Martin Hellman. Alice envoie à Bob son message secret dans un coffret qu'elle a verrouillé à l'aide d'un cadenas dont elle est la seule à posséder la clé. Bob, à la réception du coffret, ajoute au coffret son propre cadenas et renvoie le coffret à Alice, qui le reçoit donc muni de deux cadenas. Elle retire le sien, ne laissant que celui de Bob. Puis elle renvoie le coffret à Bob qui peut l'ouvrir et prendre connaissance du message, puisqu'il est détenteur de la clé du seul cadenas qui

verrouille le coffret. À aucun moment, un employé indélicat ne peut prendre connaissance du secret d'Alice.

Cette historiette prouve qu'il existe une suite d'opérations qui assure la transmission d'un message secret sans échange de clés. Ainsi, l'antique nécessité de la distribution de clés est mise hors jeu. Deux personnes qui ne se sont jamais rencontrées ou qui n'ont jamais échangé d'informations peuvent s'envoyer un message qui restera secret, même s'il passe par un canal non sécurisé.

Après avoir élaboré ces principes, Diffie et Hellman cherchent à les mettre en œuvre eux-mêmes, mais ils ne parviennent pas à trouver un équivalent cryptographique à cet échange de coffret à deux cadenas.

Le système cryptographique à clé publique RSA

En 1977, trois mathématiciens américains, Ronald Rivest, Adi Shamir et Leonard Adleman, trouvent un système asymétrique qui reste le meilleur et le plus utilisé à ce jour : le système RSA (nommé à partir des initiales des trois auteurs).

Supposons que Bob attende un message d'Alice. Nous allons expliquer en trois étapes ce qui doit être fait.

Création de la clé RSA

Bob opère de la manière suivante.

1) Il détermine au hasard deux nombres premiers p et q distincts.
2) Il calcule $n = p\,q$ et $\varphi(n) = (p-1)\,(q-1)$.
   L'entier n s'appelle le **modulo RSA**.
3) Il choisit un entier e tel que $1 < e < \varphi(n)$ et $\operatorname{pgcd}\big(e, \varphi(n)\big) = 1$.
   En général, on choisit le nombre e le plus petit possible.
   L'entier e s'appelle l'**exposant d'encryptage RSA**.
4) Il résout l'équation diophantienne $e\,x + \varphi(n)\,y = 1$ ou recourt à l'exercice 6.11 pour déterminer l'unique entier d tel que $1 < d < \varphi(n)$ et $e\,d \equiv 1 \mod \varphi(n)$.
   L'entier d s'appelle l'**exposant de décryptage RSA**.
5) Il publie dans un annuaire le couple (n, e), appelé **clé publique RSA**, et garde secrets les nombres p, q et d, qui constituent la **clé secrète RSA**.

7.2 Bob choisit sa clé RSA en prenant $p = 11$ et $q = 23$.

1) Calculer n et $\varphi(n)$.
2) Quel est le plus petit exposant d'encryptage RSA que Bob peut choisir ?
3) Quel est l'exposant de décryptage RSA correspondant ?
4) Quels nombres constituent la clé publique et la clé secrète de Bob ?

Encryptage RSA

Si Alice veut envoyer un message à Bob, elle doit procéder comme suit :

1) Elle prend connaissance de la clé publique (n, e) de Bob.
2) Elle traduit chaque lettre du texte en clair en un équivalent numérique adéquat (le code ASCII par exemple). Elle partage les chiffres de ce message en blocs de même taille.
3) Elle encrypte chaque bloc m séparément en calculant $c \equiv m^e \mod n$.
4) Elle envoie chaque bloc c à Bob.

7.3 Alice a pris connaissance de la clé publique de Bob : $(253, 3)$. Elle veut lui envoyer le message SALUT.

1) Elle numérise son message selon le code suivant :

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

   Quelle est la transcription numérique de son message en clair ?
2) Si elle divise son message en blocs de 2 chiffres, quel message crypté envoie-t-elle à Bob ?

Décryptage RSA

Théorème RSA *Soient (n, e) une clé publique RSA et d la clé secrète RSA correspondante. Alors $(a^e)^d \equiv a \mod n$ pour tout entier a.*

7.4 Le but de cet exercice est de prouver le théorème RSA.
On rappelle que $e\,d \equiv 1 \mod \varphi(n)$ et que $\varphi(n) = (p-1)\,(q-1)$.

1) Montrer qu'il existe un entier $k \geqslant 0$ tel que $(a^e)^d = a\left(a^{\varphi(n)}\right)^k$.
2) (a) Supposons $p \nmid a$ et $q \nmid a$.
   Établir que $(a^e)^d \equiv a \mod n$ grâce au théorème d'Euler.
   (b) Supposons $p \mid a$ et $q \nmid a$.
      i. Vérifier que $a \equiv 0 \mod p$ et en tirer que $(a^e)^d \equiv a \mod p$.
      ii. Montrer que $(a^e)^d \equiv a\left(a^{(q-1)}\right)^{k\,(p-1)} \equiv a \mod q$ à l'aide du petit théorème de Fermat.
      iii. Conclure que $(a^e)^d \equiv a \mod n$, grâce à l'exercice 4.4.
   (c) Supposons $p \nmid a$ et $q \mid a$.
   Montrer, de même que précédemment, que $(a^e)^d \equiv a \mod n$.
   (d) Supposons $p \mid a$ et $q \mid a$.
   Vérifier que $a \equiv 0 \mod n$ et en déduire que $(a^e)^d \equiv a \mod n$.

En vertu du théorème RSA, lorsque Bob reçoit le message codé c, il utilise sa clé privée d pour calculer $c^d \mod n$ et obtenir ainsi le message décodé.

7.5 Bob reçoit le message crypté 13 00 66 157 28 d'Alice. Déchiffrer ce message.

7.6 Crypter le message m en utilisant le système RSA avec les données suivantes :

1) $p = 3 \quad q = 11 \quad e = 7 \quad m = 5$
2) $p = 7 \quad q = 11 \quad e = 17 \quad m = 8$
3) $p = 17 \quad q = 31 \quad e = 7 \quad m = 2$

puis retrouver m à partir du message crypté.

7.7 Effectuer le chiffrement du message SOS en utilisant le système RSA de clé publique $(3233, 17)$, puis retrouver SOS à partir du message crypté.

Indication : $3233 = 53 \cdot 61$

7.8 Un système RSA a pour paramètres $p = 97$ et $q = 109$. Parmi les nombres ci-dessous, lesquels peuvent être choisis comme clé publique d'encryptage :

1) $e = 123$ 2) $e = 865$ 3) $e = 169$

7.9 Un professeur envoie votre moyenne de cryptographie au secrétariat via un courriel crypté en RSA. La clé publique du secrétariat est $(55, 7)$ et le message crypté envoyé est 25. Quelle est votre moyenne ?

7.10 Un ennemi intercepte le message chiffré $c = 10$, dont le destinataire possède la clé publique $(35, 5)$. Quel est le texte clair m ?

Sécurité du système RSA

Supposons qu'un intrus intercepte le message c et cherche à le décrypter. Il connaît aussi la clé publique, à savoir les nombres n et e. En revanche, il ne connaît pas d. Pour découvrir ce nombre, il doit trouver p et q.

En effet, la seule façon connue de découvrir d en connaissant n et e est de factoriser n pour connaître $\varphi(n) = (p-1)(q-1)$, et de calculer ensuite la solution de l'équation $e\,d \equiv 1 \mod \varphi(n)$.

La difficulté vient de ce que la factorisation de n est une tâche impossible à effectuer en un temps raisonnable, dans l'état des connaissances actuelles, pour autant que n soit suffisamment grand. On prend aujourd'hui des premiers p et q tels que leur produit soit un nombre s'écrivant avec plus de 200 chiffres. Le système est donc sûr, du moins tant que l'on ne découvre pas un algorithme rapide pour factoriser les entiers.

Authentification par signature

La cryptographie à clé publique permet également de résoudre le problème de l'authenticité et de l'intégrité des informations transmises. Imaginons par exemple qu'Alice possède un compte dans une banque administrée par Bob. Elle veut envoyer par courriel l'ordre de payer la somme de 100000 francs à l'un de ses créanciers. La banque a deux problèmes à résoudre :

1) Comment convaincre Bob que c'est bien Alice qui est l'expéditrice et non pas un escroc qui aurait usurpé l'identité d'Alice ? Ou encore, comment empêcher qu'Alice nie après coup avoir donné un tel ordre ?
2) Comment Bob peut-il être sûr que c'est bien 100000 francs qu'il faut verser à un tel et non 50000 francs à tel autre ? Un intrus n'aurait-il pas pu modifier le message ?

Montrons comment le système à clé publique RSA permet de résoudre ces problèmes.

Phase de signature et d'encryptage (par Alice)

Pour envoyer un message signé m à Bob, Alice procède ainsi :

1) Elle crypte m au moyen de sa clé privée d_A : $d_\mathrm{A}(m) = s$. L'expression s est la **signature** du message m et le couple (m, s) est le **message signé** par Alice.
2) Elle crypte le message signé (m, s) à l'aide de la clé publique e_B de Bob et lui envoie le couple $\big(e_\mathrm{B}(m), e_\mathrm{B}(s)\big)$.

Phase de vérification et de décryptage (par Bob)

À la réception de $\big(e_\mathrm{B}(m), e_\mathrm{B}(s)\big)$, Bob procède ainsi :

1) Il le décrypte au moyen de sa clé privée d_B et obtient ainsi : $\Big(d_\mathrm{B}\big(e_\mathrm{B}(m)\big), d_\mathrm{B}\big(e_\mathrm{B}(s)\big)\Big) = (m, s)$.
2) Il vérifie la signature d'Alice à l'aide de la clé publique e_A d'Alice en calculant $e_\mathrm{A}(s)$. Le message provient d'Alice si et seulement si $e_\mathrm{A}(s) = m$.

7.11 Admettons qu'Alice choisisse $p_\mathrm{A} = 11$, $q_\mathrm{A} = 23$ et $e_\mathrm{A} = 3$, comme à l'exercice 7.7. Elle obtient $n_\mathrm{A} = 253$ et $d_\mathrm{A} = 147$. Sa clé publique est $(253, 3)$ et sa clé privée est $d_\mathrm{A} = 147$.

De son côté, Bob a choisi $p_\mathrm{B} = 13$, $q_\mathrm{B} = 19$ et $e_\mathrm{B} = 5$. Il obtient $n_\mathrm{B} = 247$ et $d_\mathrm{B} = 173$. Sa clé publique est $(247, 5)$ et sa clé privée est $d_\mathrm{B} = 173$.

Alice veut faire verser à Charles la somme de 111 francs. Le message en clair est donc $m = 111$.

1) Quelle est la signature s qu'Alice calcule avec sa clé privée ?
2) Quel est le message signé codé qu'elle envoie à Bob ?
3) En utilisant la clé privée de Bob, décoder le message codé par Alice.
4) Comment Bob vérifie-t-il l'authenticité et l'intégrité du message reçu ?

7.12 Supposons qu'Alice a pour clé publique RSA $(638611, 251)$. Après avoir décrypté un message envoyé par Alice, Bob obtient la paire $(11911, 341076)$. Expliquer ce qu'il doit faire pour vérifier la signature. Doit-il considérer le message comme valide ?

7.13 La clé publique d'Alice est $(437, 17)$.
Quelle est la signature du message $m = 100$?

7.14 Pour assurer l'authenticité des messages contenant les notes, le secrétariat demande au professeur de signer ses messages codés en RSA. On sait que la clé publique du professeur est $(15, 3)$ et celle du secrétariat $(77, 7)$.

1) Quel est le message envoyé par le professeur pour indiquer la note 4 ?
2) Quelle note correspond au message crypté $(41, 41)$ reçu par le secrétariat ? Ce message a-t-il vraiment été envoyé par le professeur ?
3) Le secrétariat reçoit le message crypté $(12, 27)$. Ce message a-t-il été envoyé par le professeur ?

Réponses

7.1 1) 16 2) 4 3) 69 4) 91

7.2 1) $n = 253$ $\varphi(n) = 220$ 2) $e = 3$
3) $d = 147$ 4) clé publique : $(253, 3)$
clé secrète : $(11, 23, 147)$

7.3 1) 18 00 11 20 19 2) 13 00 66 157 28

7.5 18 00 11 20 19 → salut

7.6 1) $c = 14$ 2) $c = 57$ 3) $c = 128$

7.7 2100 2549 2100

7.8 $e = 865$ et $e = 169$

7.9 5

7.10 $m = 5$

7.11 1) $s = 89$ 2) $(232, 33)$ 3) $(111, 89)$ 4) $89^3 \equiv 111 \mod 253$

7.12 Bob vérifie que $341076^{251} \equiv 11911 \mod 638611$: le message est valide.

7.13 $s = 156$

7.14

1) $(60, 60)$
2) La note est 6. Le message a été envoyé par le professeur.
3) La signature est correcte... mais le message correspond à la note 12 ?!