

Un peu de cryptographie pratique

1 Paiement sécurisé par RSA

Vous vendez des produits en ligne sur internet et proposez à vos clients un paiement sécurisé par carte bancaire. Pour cela, lorsqu'un client saisit son numéro de carte bancaire, qui consiste en 4 groupes de 4 chiffres, les trois premiers groupes sont transmis en clair tandis que le dernier groupe (noté M) est crypté. Pour ce cryptage, vous avez choisi le procédé RSA. En pratique, pour chaque client votre ordinateur tire au hasard des nombres premiers p et q (secrets) et transmet à l'ordinateur du client $n = pq$ et e inversible modulo $(p-1)(q-1)$ pour que celui-ci puisse lui transmettre $M^e \pmod{n}$. Pour le client Alice, les clés RSA sont les suivantes : $p = 101$ et $q = 103$ (secrets), $n = pq = 10403$ et $e = 3869$ (avec de tels p et q , Alice aurait du souci à se faire et mieux vaut ne pas être client chez vous!!)

1) Vérifier que e est inversible modulo $(p-1)(q-1)$ et calculer son inverse d .

2) Le numéro transmis par Alice est 1234 8765 1973 * * * * et vous recevez 1234 8765 1973 **4207** c'est-à-dire que le nombre à quatre chiffres M qui est crypté est transmis sous la forme $M^e \equiv 4207 \pmod{n}$.

Quel est le numéro de carte bancaire de votre cliente Alice ?

2 Exemple de partage de secret par le protocole de Diffie-Hellman

Alice et Bob veulent se mettre d'accord par téléphone sur le code d'accès qu'ils choisiront pour leur ordinateur commun. Ils souhaitent le faire en utilisant le protocole de Diffie-Hellman. Pour cela, ils choisissent un nombre premier p ainsi qu'un entier α primitif modulo p (c'est-à-dire dont les puissances itérées du reste modulo p prennent toutes les valeurs possibles des restes modulo p), ces deux données étant publiques. Ils choisissent alors chacun un entier quelconque, a pour Alice et b pour Bob, qu'ils gardent secrets. Alice transmet alors à Bob α^a modulo p et Bob transmet à Alice α^b modulo p . Leur code d'accès sera alors l'entier $S \in [1, p]$ vérifiant $S \equiv \alpha^{ab} \pmod{p}$.

Alice et Bob choisissent $p = 257$.

a) Déterminer les diviseurs de $p-1$.

b) Déterminer le plus petit entier $\alpha \in [1, p-1]$ qui est primitif modulo p .

c) Alice transmet à Bob $\alpha^a \equiv 196 \pmod{p}$ et Bob a choisi $b = 15$.

Quel est le nombre modulo p que Bob doit transmettre à Alice ? Quel sera le code d'accès S de leur ordinateur ?

3 Jules César et RSA

Alice doit envoyer à Bob un message chiffré selon la méthode de décalage de Jules César, de clé secrète $K \in [0, 25] \cap \mathbb{N}$. Cela signifie précisément qu'elle décale de K crans vers la droite les lettres de l'alphabet ; par exemple si $K = 3$, "a" devient "d", "b" devient "e" etc. Alice joint cette clé secrète K à son message en la cryptant à l'aide du procédé RSA. Pour cela, Bob choisit les entiers premiers $p = 17$ et $q = 19$ qu'il garde secrets (ici un secret de polichinelle compte tenu de leur petitesse!) et publie $n = pq = 323$ et $e = 5$.

a) Vérifier que e est inversible modulo $(p - 1)(q - 1)$ et calculer son inverse d .

b) Alice transmet alors à Bob le couple formé du message crypté et de la clé cryptée

$$(kxktbtci \text{ ath kprpcrth}, K^e \equiv 2(n))$$

Quelle est la clé secrète K ? Quel le message envoyé par Alice?

4 Transmission d'un secret par RSA

Vous êtes Bob et décidez avec Alice que celle-ci vous transmettra des messages cryptés par une méthode classique à clé secrète. Pour cela il est nécessaire qu'Alice vous transmette la clé secrète qu'elle a choisie. Cette clé est un mot qu'elle va vous faire parvenir sous forme cryptée par le système à clé publique RSA. Pour réaliser cela, vous devez choisir des nombres premiers p et q (secrets) et envoyer à Alice $n = pq$ et un entier e inversible modulo $(p - 1)(q - 1)$ afin que celle-ci puisse vous transmettre $M^e \pmod{n}$, où M est son message écrit sous forme d'un entier $< n$. Vous choisissez $p = 487$, $q = 491$ (secrets), $n = pq = 239117$ et $e = 216491$.

1) Vérifier que e est inversible modulo $(p - 1)(q - 1)$ et calculer son inverse d .

2) Pour vous envoyer son mot secret Alice commence par le transformer (coder) en un nombre entier par le procédé suivant : si son mot a n lettres, elle fait correspondre (en partant de la gauche) à chaque lettre, son numéro dans l'alphabet (1 pour A, \dots , 26 pour Z) ; elle obtient ainsi n entiers a_1, \dots, a_n compris entre 1 et 26, grâce auxquels elle fabrique le nombre

$$M = \sum_{i=1}^n a_i 26^{i-1}.$$

Par exemple le codage du mot "MOT" par ce procédé donnera $13 + 15 \times 26 + 20 \times 26^2 = 13923$.

Alice vous envoie $M^e \equiv 39178 \pmod{n}$

a) Combien vaut M ?

b) Quel est le mot clé choisi par Alice?