CHIFFREMENT

30 ♦◊◊ Chiffrement/Déchiffrement RSA

On considère la clef publique RSA (11, 319), c'est-à-dire pour $n = 319$ et $e = 11$.

1. Quel est le chiffrement avec cette clé du message $M = 100$?
2. Calculer d la clé privée correspondant à la clé publique e.
3. Déchiffrer le message $C = 133$.
4. Le message chiffré 625 peut-il résulter d'un chiffrement avec la clé publique ?

31 ♦◊◊ Exemples de RSA

Considérer le système RSA avec $p = 19$ et $q = 23$.

1. Calculer n et $\phi(n) = (p-1)(q-1)$.
2. Calculer l'exposant d associé à $e = 9$, puis $e = 14$.
3. Calculer l'exposant d associé à $e = 17$.

Dans le tableau ci-contre n et e sont publics :

- $n = pq$ avec p et q deux nombres premiers secrets.
- e a pour inverse d : $ed = 1 \mod (p-1)(q-1)$ qui est tenu secret.

On donne un chiffré $C = m^e \mod n$.

À vous de retrouver p, q et m.

Détailler votre méthode et vérifier votre résultat.

n	e	C
143	17	84
247	5	115
319	11	133
323	25	19
403	7	346
407	17	50
583	19	207
4717	21	2804

32 ♦♦♦ Chiffrement RSA

On utilise les notations habituelles du chiffrement RSA : N est un entier et p et q sont deux entiers premiers tels que $N = pq$. On note ϕ l'indicatrice d'Euler $\phi = \phi(N) = (p-1)(q-1)$ et e et d sont deux éléments de $\mathbb{Z}/N\mathbb{Z}$ tels que $ed = 1 \mod \phi$.

1. On souhaite utiliser l'algorithme de chiffrement RSA.
   - Comment chiffre-t-on un message m ?
   - Et comment déchiffre-t-on un message c ?
   - Parmi les entiers N, p, q, ϕ, e et d quels sont ceux qui doivent rester secrets ?
   - Montrer que la divulgation de p, q ou ϕ permet de retrouver toutes les autres valeurs privées.
2. On pose $N = 1003$ et $e = 3$.
   - Calculer p, q et ϕ.
   - Que vaut alors l'entier d associé à e ?
   - Que vaut le message chiffré c associé au message clair $m = 4$?
   - Dans ce cas particulier, est-il possible de retrouver m à partir de c sans connaître d ?
3. On pose désormais $N = 65$.
   - Donner tous les couples (e, d) possibles (on se limitera à $e < 12$ et $e \neq d$).
   - Chiffrer le message $m = 4$ en utilisant $e = 5$.
   - Vérifier le résultat obtenu en le déchiffrant à l'aide de la clef privée correspondante.

■

33 ♦♦◊ Chiffrement El Gamal

Alice choisit $p = 97$ et $g = 13$.

(a) Elle choisit aléatoirement un nombre a, disons 45, dans l'intervalle $[1, ..., 95]$.

(b) Elle calcule $\alpha = (13^{45} \mod 97) = 20$.

(c) Elle publie sa clé $(97, 13, 20)$ et garde secrète sa clé 45.

Bob veut envoyer le message `RAS` à Alice.

(a) En utilisant le code ASCII, son message est $118\,101\,119$.

(b) Il le découpe en nombres entre 0 et 97 : $11\,81\,01\,11\,09$.

(c) Il choisit aléatoirement un nombre b, disons 35, dans l'intervalle $[1, .., 95]$.

(d) Il calcule $\beta = 13^{35} \mod 97 = 71 \mod 97$.

1. Vérifier que le chiffré de son message est $(71, 21\,40\,46\,21\,26)$.
2. Comment Alice déchiffre-t-elle le message de Bob ? Déchiffrer-le.

■

34 ♦◇◇ Changement de clés

Alice change sa clé RSA tous les 25 jours. Bob lui change sa clé tous les 31 jours. Sachant qu'Alice change sa clé aujourd'hui et que Bob a changé sa clé il y a trois jours, déterminer quand sera la prochaine fois qu'Alice et Bob changeront leur clé le même jour.

35 ♦♦◇ TP pari-gp RSA

Alice veut envoyer un message secret à Bob. Bob décide d'utiliser RSA avec $p = 11^{20} + 136$ et $q = 9^{22} + 8$. Il choisit aussi $e = 12234567$, calcule $N = pq$, et donne publiquement (N, e).

1. Vérfiez que e est premier avec $(p-1)(q-1)$.
2. Nous savons que h est la huitième lettre de l'alphabet, e la cinquième etc...
   Alice souhaite envoyer $hello$, elle convertit son message et obtient $m = 0805121215$.
   Calculez le chiffré C de m qui vérifie $C = m^e \mod N$.
3. Bob reçoit C pour déchiffrer, il doit calculer d qui vérifie $ed = 1 \mod (p-1)(q-1)$. Montrez comment en utilisant la fonction `gcdext()` Bob peut déterminer d.
4. Déchiffrez C et comparez le à m.
5. Utilisez la fonction `factor()` pour montrer que le choix de Bob pour N n'était pas bon.

36 ♦♦◇ TP pari-gp factorisation

La commande `a%b` donne le reste de la division euclidienne de a par b.

Pour trouver un facteur de $N = 10^{15} + 3$ on utilise l'algorithme naïf suivant :

```
N=10^15+3;d=2;while(N%d>0,d=d+1);d;
```

1. En utilisant la commande # déterminez combien de temps celà prend-il.
2. Modifiez ce programme pour qu'il n'effectue que les divisions par des entiers impairs. Combien de temps celà prend-il ?
3. Modifiez encore ce programme pour qu'il s'arrête dès que $d > \sqrt{N}$.
   Combien de temps celà prend-il ? Expliquez pourquoi.