Université de Lille 1 SCIENCES ET TECHNOLOGIES

L1 - SESI - 2015–2016

Arithmétique et Cryptographie

DS2 – Durée 2h
13 mai 2016

Toutes les réponses doivent être justifiées et vous soignerez votre rédaction.

Les documents son interdits, ainsi que les appareils électroniques (téléphones, ordinateurs portables, etc...). Seules les calculatrices sont autorisées.

Notez le numéro de votre groupe sur la copie.

Autour de Fermat

1. Citez le petit théorème de Fermat.
2. En justifiant soigneusement, calculez $(123 \times 456)^{666} \pmod 7$ (la calculatrice n'est absolument pas nécessaire ici).
3. Citez la version **améliorée** du petit théorème de Fermat.
4. En justifiant soigneusement, donnez le chiffre des unités de 123^{456789} (là encore calculatrice non nécessaire).

On désigne par p un nombre premier et par a un entier compris entre 1 et $p-1$.

5. Quelle relation existe-t-il entre a et $a^{p-2} \pmod p$?
6. Utilisez cette relation pour réaliser une fonction en Python paramétrée par un entier $1 \leq a < p$ et un nombre premier p qui renvoie l'inverse de a modulo p.

César flotte-t-il ?

On considère comme à l'accoutumé alphabet de 26 lettres `ABC...Z` codé par A=0, B=1...

On propose l'extension *flottante* du chiffrement de César suivant. La clé est une lettre (par exemple K) ou la valeur numérique correspondante (c'est-à-dire 10). En utilisant le chiffrement de César, on chiffre la première lettre du message clair avec la clé. La deuxième lettre du message clair est alors chiffrée de ka même façon avec la première lettre du chiffré pour clé, la troisième avec la deuxième lettre du chiffré...

Ainsi le message **AVE** pour la clé **D** est chiffré en **DYC**.

7. Déchiffrez le message : **RMALFYGUH** sachant qu'il a été chiffré avec la clé **N** ?

8. Donnez au moins un avantage et au moins un (très grave) inconvénient de ce protocole de chiffrement par rapport à celui dont il est inspiré ?

Cryptographie RSA

Alice a pris connaissance de la clé publique de Bob : $(253, 3)$. Elle veut lui envoyer le message `OUI`. Elle code le message selon le code standard $A \leftrightarrow 0$, $B \leftrightarrow 1\ldots$ Elle réalise ensuite l'opération suivante :

	O	U	I
M (en clair)	14	20	08
C=M^3 mod 253	214	157	006

Le message chiffré est donc le triplet $(214, 157, 006)$.

9. Déterminez dans ce cas simple, les 2 nombres premiers p et q tels que $253 = pq$, $\phi(253)$ et la clé d de déchiffrement.

10. En utilisant l'algorithme d'exponentiation modulaire rapide, et en précisant le détail des calculs, vérifiez qu'en déchiffrant la première lettre du chiffré vous obtenez bien la lettre `O`.

11. Pourquoi cette façon de chiffrer n'est-elle pas sure ?

12. Pour pallier ce problème, Alice décide de transmettre ses messages en un seul bloc. Elle calcule donc $142008^3 \pmod{253}$. Pourquoi cette démarche ne permet-elle pas de déchiffrer le message correctement ?

13. Bob lui fait part de ce problème pour décrypter le message et ils décident alors d'utiliser les nombres premiers $p = 1931$ et $q = 1129$. Montrer que $e = 7$ peut être choisi comme exposant public de chiffrement et qu'il est possible de chiffrer le message 142008 avec la clé (pq, e).

14. Des trois nombres 1244023, 1244024, 1244025 déterminez sans calcul le seul qui puisse être la clé de déchiffrement d correspondant à la clé publique de la question précédente ?

15. En admettant que le seul candidat trouvé dans la question précédente est bien la clé de déchiffrement, donnez un encadrement du nombre de multiplications modulaires effectuées dans une opération de déchiffrement utilisant l'exponentiation rapide.