Université de Bordeaux — L3 Math, Info, Math-Info
Collège Sciences et Technologies

Année Universitaire 2014-2015
Devoir Surveillé
Parcours : IN601, MA601, MA603 **UE :** N1MA6W31
Épreuve : Cryptographie et Arithmétique
Date : 16 Mars 2015 **Heure :** 11h00 **Durée :** 1h30
Documents : Aucun document autorisé
Épreuve de M. Cerri

L'usage de la calculatrice est autorisé.

Exercice 1 [Nombres de Carmichael]

On rappelle qu'un nombre de Carmichael est un entier N composé, tel que pour tout entier a premier avec N on ait $a^{N-1} = 1 \bmod N$. Le critère de Korselt est le suivant : N est un nombre de Carmichael si et seulement si N est composé, sans facteur carré (i.e. produit de premiers distincts) et tel que si p est un premier divisant N, alors $p-1$ divise $N-1$. Dans la suite, on se servira librement de ce théorème qu'il n'est pas demandé de redémontrer.

1) Soit $k \geq 1$ un entier tel que $6k+1$, $12k+1$ et $18k+1$ soient tous trois premiers. Montrer que $N = (6k+1)(12k+1)(18k+1)$ vérifie $N = 1 \bmod 36k$ et en déduire que N est un nombre de Carmichael. Un nombre de cette forme est appelé nombre de Chernick[1].

2) Quels sont les deux plus petits nombres de Chernick ?

On se propose maintenant de prouver que les deux propositions suivantes sont équivalentes :

(1) N est un nombre de Carmichael ;
(2) N est composé et pour tout entier a, $a^N = a \bmod N$.

3) Montrer que (2) implique (1).

4) On suppose désormais que N est un nombre de Carmichael. Soient p un premier divisant N et a un entier.

a) Montrer que si p divise a, alors $a^N = a \bmod p$.

b) Montrer que si p ne divise pas a, alors $a^{N-1} = 1 \bmod p$.

c) En déduire que (1) implique (2).

On se propose finalement de démontrer qu'un nombre de Carmichael est impair et est le produit d'au moins trois premiers.

5) Supposons qu'un nombre de Carmichael N soit pair. Montrer qu'il existe un premier p impair divisant N et que l'on ne peut pas avoir $p-1 \mid N-1$.

6) Retrouver ce résultat (N est impair) en utilisant la définition d'un nombre de Carmichael et un a approprié.

7) Supposons qu'un nombre de Carmichael N soit produit de deux premiers impairs distincts p et q. Montrer que $p-1 \mid q-1$ et aboutir à une contradiction.

[1] On sait qu'il existe une infinité de nombres de Carmichael. En revanche, on ne sait pas s'il en est de même pour les nombres de Chernick.

Exercice 2 [Théorème chinois]

1) Montrer que 7 est inversible modulo 110 et calculer son inverse.
2) Soit $N = 3^{1000}$. Montrer que

$$\begin{cases} N &= 1 \mod 2 \\ N &= 1 \mod 5 \\ N &= 4 \mod 7 \\ N &= 1 \mod 11 \end{cases}$$

3) En déduire que $N = 1 \bmod 110$.
4) Quel est le reste de la division euclidienne de 3^{1000} par 770 ?

Exercice 3 [RSA]

Alice et Bob communiquent à l'aide du protocole RSA. La clé publique de Bob est $(N, e) = (81070877, 127)$. Bob a oublié les premiers p et q à l'aide desquels il avait déterminé N ainsi que sa clé privée d, mais il se rappelle que $\phi(N) = 81052860$.
1) Retrouver p et q.
2) Retrouver d.
3) En quoi le choix des premiers p et q est maladroit ? Montrer comment Oscar peut les retrouver rapidement. Détailler ses calculs.

Exercice 4 [Vers AKS]

Soit n un entier > 1. Si deux polynômes $P(X), Q(X) \in \mathbb{Z}[X]$, l'anneau des polynômes à coefficients entiers, on écrira $P(X) = Q(X) \bmod n$ pour exprimer que n divise tous les coefficients de $P(X) - Q(X)$. Soit $a \in \mathbb{Z}$ tel que $\text{pgcd}(a, n) = 1$. On se propose de démontrer que n est premier si et seulement si $(X + a)^n = X^n + a \bmod n$.
1) Montrer que si n est premier, on a bien $(X + a)^n = X^n + a \bmod n$.
2) Réciproquement, supposons que n est composé. Soient p un diviseur premier de n et $k \geq 1$ tel que $p^k \mid n$ et $p^{k+1} \nmid n$.
a) Montrer que $p^{k+1} \nmid n(n-1)\cdots(n-p+1)$.
b) En déduire que $p^k \nmid \binom{n}{p}$.
c) Montrer que $(X + a)^n \neq X^n + a \bmod n$.