Année universitaire 2014-2015
Licence 3 de mathématiques
Cryptographie et arithmétique - Feuille 4

Exercice 1

Soient n et a deux entiers ≥ 2. Prouver que $2n$ divise $\varphi(a^n + 1)$.

Exercice 2

Notons C l'ensemble des entiers de la forme $p^r m$ avec p premier, $r \geq 1$ et $m \in \{1; 2\}$. Soit n un entier ≥ 2 tel que $n \notin C$.

a. Montrer qu'il existe $b \geq 3$, $c \geq 3$ et $a \in \{1; \cdots; n-1\}$ vérifiant : $n = bc$, b et c sont premiers entre eux, b divise $a + 1$ et c divise $a - 1$.

b. Démontrer que $2 \leq a \leq n - 2$ et que $a^2 \equiv 1 \bmod n$.

c. Soit α un entier vérifiant : $2 \leq \alpha \leq n - 2$ et $\alpha^2 \equiv 1 \bmod n$. Comment trouver un facteur non trivial de n à l'aide de α ?

Exercice 3

Soient m et n deux entiers ≥ 1. Prouver que m et n sont premiers entre eux si et seulement si $m^{\varphi(n)} + n^{\varphi(m)} \equiv 1 \bmod mn$.

Exercice 4

On considère k personnes $B_1, \cdots, B_k$ ayant pour clefs RSA publiques respectives $(n_1; e), \cdots, (n_k; e)$, avec le même exposant public e. Désignons par P le ppcm de $n_1, \cdots, n_k$.

Alice envoie les chiffrés d'un même message m à tous les B_i. Montrer qu'un attaquant peut déterminer m si $m^e < P$ (*indication :* considérer m^e modulo P).

Exercice 5

Bob a choisi la clef RSA publique $(n; e_B)$ et Catherine la clef $(n; e_C)$, avec le même module n.

a. On suppose e_B et e_C premiers entre eux. Alice envoie les chiffrés d'un même message m à Bob et à Catherine. Comment l'attaquant Oscar peut-il obtenir m ?

b. Supposons $n = 221$, $e_B = 11$ et $e_C = 7$. Oscar intercepte les chiffrés 210 et 58 à destinations respectives de Bob et de Catherine. Retrouver le message m.

Exercice 6 : critère de Korselt

Soient m et n deux entiers ≥ 2. Montrer que les propriétés suivantes sont équivalentes :
(α) Pour tout entier a, n divise $a^m - a$;
(β) Pour tout premier p divisant n, p^2 ne divise pas n et $p - 1$ divise $m - 1$.

Prouver que 561 divise $a^{561} - a$ pour tout $a \in \mathbb{Z}$.

Exercice 7 : chiffrement d'Elgamal

Soit n un entier ≥ 1. Soit $g \in (\mathbb{Z}/n\mathbb{Z})^*$ un élément d'ordre d. Soit x un entier ; posons $h = g^x$. Pour chiffrer un message $m \in (\mathbb{Z}/n\mathbb{Z})^*$, on choisit un entier r et on calcule $(c_1; c_2) = (g^r; h^r m)$.

a. Quelle est la clef publique de ce cryptosystème ? Combien un message clair a-t-il de chiffrés possibles ?

b. Calculer c_1^x. En déduire la clef privée et la fonction de déchiffrement D.

c. Vérifier que D est un morphisme de groupes.

Exercice 8

Soient $n \geq 2$ et a deux entiers premiers entre eux.

a. Supposons n premier. Montrer la congruence $(X + a)^n \equiv X^n + a \bmod n$.

b. Soit p un facteur premier de n. Prouver que $p^{v_p(n)}$ ne divise pas C_n^p.

c. Supposons que $(X + a)^n \equiv X^n + a \bmod n$. Démontrer que n est premier.