Université Bordeaux
Mathématiques, Informatique

M1 CSI, Cryptologie
Année 2019 – 2020

FEUILLE D'EXERCICES n° 7

Clé publique (2)

Exercice 1 – Montrer que si C est le chiffré d'un message M par un chiffrement RSA modulo n, alors on peut facilement calculer $\left(\frac{M}{n}\right)$ à partir de C.

Exercice 2 –

1) Calculer les symboles de Jacobi $\left(\frac{37}{209}\right)$ et $\left(\frac{79}{209}\right)$. Les éléments 37 et 79 sont-ils des carrés modulo 209 ?

Soient p et q deux premiers impairs distincts. On pose $n = pq$.

2) Combien y a-t-il d'éléments $x \in \{0, 1, \ldots, n-1\}$ vérifiant $\left(\frac{x}{n}\right) = 0$?

3) Même question avec 1 et -1 à la place de 0.

4) Parmi les x vérifiant $\left(\frac{x}{n}\right) = 0$, combien sont des carrés modulo n ?

5) Même question avec 1 et -1 à la place de 0.

Exercice 3 – Déterminer les racines carrées de 56 dans $\mathbb{Z}/143\mathbb{Z}$.

Exercice 4 – Alice utilise le système de Rabin. La clé publique d'Alice est $n = 1772117$. Ève procède à une attaque à chiffré choisi. Elle a accès à un oracle de déchiffrement qui prend en entrée un chiffré $C \in \{x^2 \bmod n\ ;\ 0 \leqslant x \leqslant n-1\}$ et retourne une de ses racines carrées modulo n. Elle soumet $C = 5000^2 = 190362 \bmod n$ et obtient 458860. Aider Ève à retrouver la clé secrète (p, q) d'Alice.

Exercice 5 – En partant de $x_0 = 2^2$, écrire sur une période la suite résultant du générateur de Blum Blum Shub modulo 209. Comparer le nombre de 1 et le nombre de 0, ainsi que la distribution des couples de symboles consécutifs.

Exercice 6 – Bob utilise un système de Blum-Goldwasser. Sa clé publique est $n = 253$, sa clé secrète est $(11, 23)$. Il reçoit le chiffré $C = (0001101, 234)$. Qu'obtient-il à l'issue du déchiffrement ?

Exercice 7 – Un clair M est chiffré en $C = (c, x)$ par un système de Blum-Goldwasser de clé publique n. Oscar intercepte C. Supposons qu'il a le droit de demander à déchiffrer un $C' \neq C$ de son choix. Montrer comment, en choisissant bien C', il peut retrouver M.