Université Paris 8 Année 2021–2022

M1 Mathématiques et applications, parcours ACC et CSSD

Cryptographie à clef publique – Devoir semaine 2

devoir du 04/02/2022
à rendre jusqu'au 11/02/2022

Exercice 1. RSA brut avec clairs liés (4 points).

On considère le chiffrement RSA dans son mode de fonctionnement « brut ». On note $n = pq$ le module public. **On suppose que l'exposant public est $e = 3$.**

On chiffre successivement les messages m, $m+1$ et $m+2$ où $m \in \mathbb{Z}/n\mathbb{Z}$.

Question 1.– Donner (en fonction de m) la valeur des chiffrés c_0, c_1 et c_2 correspondant respectivement aux messages m, $m+1$ et $m+2$.

Question 2.– Comment un attaquant passif peut-il retrouver le message m en effectuant des combinaisons linéaires des chiffrés c_0, c_1 et c_2 ?

On fixe maintenant un entier $r \in (\mathbb{Z}/n\mathbb{Z})^\times$, que l'on suppose public. On chiffre ensuite les messages z et $z+r$ où $z \in \mathbb{Z}/n\mathbb{Z}$.

Question 3.– Expliquer comment, avec grande probabilité sur la valeur de z, un attaquant passif peut retrouver la valeur de z à partir des chiffrés de z et $z+r$.

Exercice 2. Utilisation de RSA brut pour une procédure de vote (1 points).

Dans une procédure de vote, on utilise le système de chiffrement RSA dans son mode de fonctionnement « brut ».

On suppose qu'il y a K candidats, où K est une petite constante. L'autorité qui organise le vote publie une clé publique RSA (n, e), et assigne au i-ème candidat une valeur aléatoire $m_i \in \mathbb{Z}/n\mathbb{Z}$, de telle sorte que les valeurs $m_1, \ldots, m_K$ soient mutuellement distinctes.

Pour voter pour le i-ème candidat, un élécteur doit chiffrer m_i avec la clé publique de l'autorité, puis envoyer à l'autorité le chiffré correspondant c_i. L'autorité déchiffre ensuite le vote de chaque électeur pour comptabiliser le nombre de votes.

Dans cet exercice, on ne s'intéresse pas à la non-confidentialité du vote du point de vue de l'autorité.

Question 1.– Expliquer comment un attaquant passif, qui observe les échanges entre un électeur et l'autorité de vote, peut néanmoins savoir pour qui l'électeur a voté.