1 Cryptosystème El-Gamal

Hypothèse Décisionelle de Diffie-Helmann

1. Rappeler l'hypothèse décisionnelle de Diffie-Hellman.
2. Si l'hypothèse n'est pas vérifiée, comment un attaquant peut-il retrouver le message ?

Propriété d'homomorphisme

1. Montrer qu'en connaissant le chiffré d'un message m il est possible de chiffrer le message $2m$.
2. Connaissant le chiffrer de deux messages m_1 et m_2, peut-on chiffrer $m_1 + m_2$? Et $m_1 \times m_2$?

2 Paradoxe des anniversaires

Soit N un entier et $0 \leq p \leq 1$ une probabilité. On tire n éléments aléatoirement dans l'ensemble $\{1, 2, ..., N\}$. Quel est la probabilité de tirer deux fois le même élément ?

3 Algorithmes classiques

1. En utilisant la méthode Pas de bébé, pas de géant calculer le logarithme discret de 17 en base 5 dans $\mathbb{Z}/73\mathbb{Z}$.
2. En utilisant la méthode de Pollard-rho calculer le logarithme discret de 66 en base 11 dans $\mathbb{Z}/79\mathbb{Z}$.