Sécurité prouvable
TD Chiffrement à clé publique

Exercice I

1. Rappelez la syntaxe et le fonctionnement (correctness) des schémas de chiffrement à clé publique.
2. Dans le chiffrement Elgamal, on travaille dans un groupe cyclique multiplicatif généré par g, un générateur d'ordre premier q, dans le corps fini F_p pour un grand nombre premier p. La clé privée est un entier $sk \in \{1, \dots, q-1\}$, tandis que la clé publique est $g^{sk} \bmod p$. Pour le chiffrement, il faut premièrement choisir un nombre aléatoire r et calcule $C_1 = g^r \bmod p$ et $C_2 = m \cdot pk^r \bmod p$.
    a. Comment peut-on déchiffrer un texte chiffré par la méthode de Elgamal ?
    b. Pouvez-vous instancier la syntaxe PKE par le chiffre de Elgamal ?

Exercice II

Écrivez des jeux et des définitions de sécurité pour les hypothèses suivantes : DLog, CDH, DDH.

Ensuite rappelez le jeu de sécurité IND-CCA2.

Exercice III

La notion de sécurité IND-CPA est similaire à la notion IND-CCA2, sauf que l'attaquant n'a accès à aucun oracle de déchiffrement.

1. Prouvez la sécurité IND-CPA du chiffre de Elgamal. Sous quelle(s) hypothèses cette sécurité tient-elle ?
2. Pouvez-vous montrer une attaque IND-CCA2 contre Elgamal ?