

Exercise (Security of ElGamal implies Decisional Diffie Hellman). *Show that ElGamal cryptosystem is (t, ε) -IND-CPA secure only if the underlying group \mathbb{G} is Decisional Diffie Hellman group.*

Solution.