Elgamal Public Key Encryption (1989)

Parameter Generation: This step generates system-wide keys.

Let G be a Probabilistic Polynomial Time algorithm, \((p, q, g) \in \mathbb{G}(1^k)\),

where \(k\) is a security parameter.

\[ a) \quad (p, q) \text{ are primes with } \vert q \vert > \frac{k}{2} \text{ and } q|(p-1) \text{ and } q^2 \not| (p-1) \]

\[ b) \quad g \text{ is a generator of the subgroup of } \mathbb{Z}_p^* \text{ having order } q \]

Strong primes, Sophie-German primes

\[ \text{If } q \text{ is prime, } p = 2q + 1 \] 

\[ \text{DL-problem appears to be hard.} \]