El Gamal Cryptosystem

The El Gamal cryptosystem is a public key cryptosystem based on the computational difficulty of computing discrete logarithms in cyclic groups.

The cryptosystem is defined over a group G_q of order q with generator g. The secret key x is chosen randomly in $\mathbb{Z}_q$ and the public key y is created as follows

$$y = g^x$$

Encryption of a plaintext $m \in G_q$ is done by choosing a random $s \in \mathbb{Z}_q$ and computing

$$(u, v) = (g^s, y^s m) \in G_q \times G_q$$

Decryption of a ciphertext $(u, v) \in G_q \times G_q$ is achieved by using the private key x to compute

$$u^{-x}v = (g^s)^{-x}y^s m = (g^x)^{-s}y^s m = y^{-s}y^s m = m$$

The El Gamal Cryptosystem possesses a homomorphic property. This means that the encryption of the product of two plaintext messages is the same as the product of the individual encryptions of the plaintexts. The randomnesses is replaced by the combined randomness of the individual encryptions. By choosing one of the messages to the identity element in the group one has obtained the ability to reencrypt a particular ciphertext without knowing the original plaintext nor the randomness. This property of a cryptosystem is necessary if it should be used in a reencryption mix-net.

Security

The security of the El Gamal cryptosystem relies on the Decisional Diffie-Hellman assumption. The assumption is closely related to the discrete logarithm in cyclic groups.

The discrete logarithm is a generalization of the usual logarithm to groups. Let $b = g^a \in G_q$ where $a \in \mathbb{Z}_q$, then a is said to be the discrete logarithm of b in the group G_q. There is currently no known efficient classical algorithm that given (G_q, g, b) is able to calculate a in a reasonable amount of time (polynomial time). The discrete logarithm problem is thus considered to be a hard problem.

The Decisional Diffie-Hellman assumption concerns a problem related to the discrete logarithm. The assumption in a certain group G_q means that if $a, b, c \in \mathbb{Z}_q$ are chosen randomly, every efficient algorithm, on input g^a, g^b and $y \in \{g^{ab}, g^c\}$, is unable to tell if $y = g^{ab}$ or $y = g^c$.

The security of the El Gamal cryptosystem relies on the Decisional Diffe-Hellman assumption in finite cyclic groups G_q. This means that the El Gamal cryptosystem is secure as long as the assumption is true.