Elgamal Cryptographic System

Team 3: Abdul Body, Haya Alruqi, Josh Kelley, Seth Wilson

The Elgamal Cryptographic System is a public key cryptosystem that was published in 1985 by Taher Elgamal in a paper titled, “"A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms.”1 Public key encryption systems use asymmetric encryption algorithms that rely on one key that is publicly distributed, commonly called a public key, and a different but related key that is kept secret, commonly called a private key.2

Whitfield Diffie and Martin Hellman described a number of requirements for public key cryptographic algorithms. The two requirements they identified for the key pair are that it is computationally easy to generate a key pair and that it is computationally infeasible for an adversary to determine the private key from knowledge of the public key.3

The key pair in the Elgamal Cryptographic System is based on the choice of a prime number *q* and a number alpha, a primitive root of *q*.4 A private key value is chosen and the public key value is the remainder modulus *q* of alpha raised to the power of the private key. To obtain the private key value from the public key, an adversary would have to solve the difficult problem of computing a discrete logarithm, which is thought to be computationally infeasible for values of *q* that are at least 300 decimal digits in length.5

In order to encrypt a message, the sender will use the public key information that they received. Requirement two for Public-Key Encryption states “It is computationally easy for a sender A, knowing the public key and the message to be encrypted, M, to generate the corresponding ciphertext.”6 This is easy to do with the Elgamal Cryptography system. The sender first decides on the message M they want to send. This may need to be broken up into multiple blocks based on the rule that the integer value of the message block must be less than the prime number q value that was passed in the public key. With this message broken up into block the sender then needs to select a random integer k that also must be less than the value of q. With M and k, the sender will then use these values and the those of the public key to calculate a cipher pair per message block. The sender will then send the cipher messages to the receiver in the form of (C1, C2).

Another requirement for the cryptology system is that “It is computationally infeasible for an adversary, knowing the public key, PUb, to determine the private key, PRb.”7 The random value of k is chosen to aid in the encryption process which means that Elgamal also meets this requirement by adding another variable along with the public key to make a private key. By picking a new value of k for every message block it makes it so that even if a person is able to guess one k value, they would still not be able to decrypt the entire message. This helps this system in meeting the requirement that “It is computationally infeasible for an adversary, knowing the public key, PUb and a ciphertext, C, to recover the original message, M.”8

For decryption of Cipher text in the Elgmal Cryptographic System we have the following steps. First receive cipher text C1 and C2 in these we have the ciphertext that we get when we done the encryption and then we will Calculate the K by using the given formula:

K=C(xa) mod q.

By using this formula, we will calculate the value of K which will be put later in the equation of M. The value of K we can use it only one time. After calculating the value of K, we will then decrypt the cipher text. For decrypting plain text, we used the following formula:

M=(C2)K-1 mod q.

In the M we will get the decrypted plain text. In this formula K is multiplied by C2 and then take mod with q and after that we will receive the cipher text.

An application of the ElGamal is electronic signatures. Electronic signatures need to be secure since they serve the same purpose as traditional signatures. Electronic Signatures are tied to documents using mathematics so that they cannot be replaced or copied into another document. Elgamal is one successful method of creating, verifying, and protecting signatures from forgery.

Public key cryptosystems like Elgamal are useful for e-signatures because the signature is created with private information but verified with public information. The signing protocol consists of the set up, signing the message, and verification. The set up is similar to the encryption process. The user selects a large prime number and secret integer. When signing the message, the random integer k is selected and the public key is computed. Users should avoid repeating the integer for k to ensure security. During verification, the message is decrypted using public information to determine the signature’s validity.

1. <https://en.wikipedia.org/wiki/ElGamal_encryption#cite_note-1>. Accessed 12/1/2019.

2. Stallings, *Cryptography and Network Security*, p. 274.

3. Ibid.

4. Id., p. 301.

5. Id., p. 303.

6. Id., p. 274.

7. Ibid.

8. Id., p. 275.

Grewal, J. (2015 Sept, 30). Elgamal: Public-Key Cryptosystem. Retrieved from http://cs.indstate.edu/~jgrewal/steps.pdf

Davies, I. and Dhandhania, K. Digital Signatures: ElGamal Signature Scheme and Digital Signature Algorithm (and Birthday Attacks). Retrieved from https://www.commonlounge.com/discussion/35a1c2baa00b447f9275e8f71b02ef29