Topic: Attacks on ElGamal
Student: Tihana Britvić, 70078007

Introduction:

Public key cryptosystems have an elegant mathematical simplicity, however, it is often the case that a simple implementation is not secure. In particular, in this paper, I will describe several attacks on ElGamal and RSA which work well when the encrypted message is short and has not been preprocessed. The attacks on ElGamal depend on the parameters, which are commonly used in practical implementations, and are also used while creating the cryptosystem. The formalization of an idea of what makes a secure cryptosystem is a popular subject among computer scientists. However, formal definitions are sometimes a bit stronger than necessary for practical security regarding a fact that many cryptosystems being used in practice do not satisfy the formal definitions. ElGamal cryptosystem implementation is something that is often referred to in this context. In this paper, I will discuss the worthiness of attacks that strive to formal definitions of security in actual implementations.

Body:

- Implementation of system
  - Definiton of system
  - Symmetric/Public key cryptosystems

- ElGamal cryptosystem
  - Encryption and Decryption
  - Security and Efficiency
  - Brute Force Attacks
- Meet-In-The Middle Attack
  - Assumptions
  - Attack
  - Solution collision
  - Implementation
- Two Table Attack
  - Definition and solution
  - Implementation
  - Memory and time estimation

Conclusion:

In this paper attacks which rely on the underlying mathematics will be discussed. Timing attacks will be discovered against various cryptosystems. Implementing a cryptosystem securely requires far more than an understanding of the basic algorithm. Secure implementation is difficult, and using an existing implementation which has already undergone extensive public review should always be preferred over creating a new implementation. While implementing we must be aware of possible attacks on the system, and choose keys and parameters to make those attacks infeasible.

References:

- Stinson, Cryptography: Theory and practice
- Abdalla, Bellare, and Rogaway: An encryption scheme based on the Diffie-Hellman problem
- N. A. Howgrave-Graham and N. P. Smart. Lattice attacks digital signature schemes