République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la
Recherche Scientifique
Ecole supérieure d'informatique

Mémoire de fin d'études

Pour l'obtention du diplôme de Master 2 en Informatique

Option : ingénierie des systèmes informatiques

A Shared Secret Key Diffie-Hellman Protocol enhancements to withstand Man-in-the-Middle Attack

---

Réalisé par

M. Mansour Aboubaker

Encadré par: Dr. Amina Souyah (ESI-SBA)

Date de soumission: / /2023

Abstract

One of the most famous key exchange protocols is Diffie-Hellman Protocol (DHP) which is a widely used technique on which key exchange systems around the world depend. This protocol is simple and uncomplicated, and its robustness is based on the Discrete Logarithm Problem (DLP). Despite this, the protocol is vulnerable to the Man-in-the-Middle (MitM) attack. The scope of this thesis is to provide a relevant review on secure key exchange mechanisms that are employed in practice to deal with the issue of sharing securely the secret key between the authorized partied in symmetric cryptosystems.

On the other hand, the theory aspect of this thesis is concerned about Comprehensive review and definitions about previous concepts of cryptography and its types. It also give a comprehensive idea about the classical Diffie Hellman protocol and its problem with exchanging keys. Moreover, the thesis includes some previously studied approaches which provided different solutions to this above mentioned problem and the method used to reach it.

Keywords: Cryptography, Secret key exchange, Diffie-Hellman Protocol (DHP), Man-in-the-Middle (MitM) attack.
