UNIVERSITI TEKNOLOGI MARA

TECHNICAL REPORT

THE BINARY EXPONENTIATION AND MODULAR MULTIPLICATION IN DIFFIE HELLMAN KEY EXCHANGE

NURIN AISYAH BINTI AZMAN – 2019257192
NURUL HAZIRAH BINTI AZIZ – 2019406004
WAN NUR AKLIEMA BINTI WAN MUHAMMAD SUKRI – 2019423216
(P25M22)

Report submitted in partial fulfillment of the requirement for the degree of
Bachelor of Science (Hons.) (Computational Mathematics)
Faculty of Computer and Mathematical Sciences

AUGUST 2022

ACKNOWLEDGEMENTS

IN THE NAME OF ALLAH, THE MOST GRACIOUS, THE MOST MERCIFUL

Firstly, we are grateful to Allah S.W.T for giving us the strength to complete this study successfully.

We would like to express our greatest gratitude to our supervisor, Miss Nur Lina Binti Abdullah for providing invaluable guidance and feedback throughout this study. Her consistent support, encouragement and patience carried us through all stages of writing our study. We would also like to thank our Cryptography lecturer, Mr. Md Nizam bin Udin for teaching this subject to us and classmate. His knowledge helped us to complete our study easily and effectively on time. Besides, we would like to extend our heartfelt thanks to all our group members.

TABLE OF CONTENTS

ABSTRACT

Numerous approaches to establish secure communication have emerged with the advancement of modern technology to ensure the shared secret are protected from attackers. Protocols for authenticated key exchange serve a significant role in communication security and are widely used in a variety of real-world network applications. Recent study suggests using modular multiplication instead of exponentiation operation in Diffie-Hellman Key Exchange to securely generating the common session key. However, the processes are not properly discussed. Therefore, the process of applying the Left-to-Right Binary method to compute modular exponentiation that are frequently used in Diffie-Hellman Key Exchange protocol are briefly discussed. Further, our key objective is to develop a mathematical equation using a combination of modular exponentiation and modular multiplication that satisfies the condition of Diffie-Hellman Key Exchange protocol with eight parties. Therefore, in this study we used Left to Right Binary method to compute the common session key, k in Case 1 and each of the participants' private key in Case 2. As a result, we managed to modify the mathematical equation using a combination of modular exponentiation and modular multiplication, hence making it difficult for an attacker to break into the system since the intruder or any attacker needs to find eight different private keys. In the further, this study can be extended by increasing the number of parties involved which will make any users communicate with each other. Besides that, this study should be repeated using a bigger value for both private key and prime number. Other than that, upcoming research can modify the mathematical equation in either case 1 or case 2 to make sure that the value of the common key is equal. Reason for this is that the LRB method can be applied everywhere in Diffie-Hellman Key Exchange that offers more flexibility if the common key is equal for both cases. Lastly, this study uses numerical example for proving, hence further work may prove the proposed method by computation time for efficiency.