UNIVERSITI TEKNOLOGI MARA

TECHNICAL REPORT

MATHEMATICAL MODELLING OF RSA CRYPTOSYSTEM BASED ON MODIFICATION OF MODULAR EXPONENTIATION WITH HESSIAN CURVE

NURUL HUSNINA AMANI BINTI ABD HALIM (2021178613)

NUR HAZIRAH BINTI MOHD SUKHAIMI (2021119429)

NUR ASYIKIN BINTI MOHD RADZIR (2021103419)

P18S22

Report submitted in partial fulfillment of the requirement
for the degree of
Bachelor of Science (Hons.) (Mathematics)
College of Computing, Informatics, and Media

FEBRUARY 2023

ACKNOWLEDGEMENTS

In the name of Allah, the most gracious, the most merciful. First and foremost, we are thankful to Allah S.W.T for giving us the strength, knowledge, ability, and opportunity to complete this technical report successfully. Secondly, we owe deep gratitude and appreciation to the supervisor, Miss Nur Lina Abdullah and the lecturer, Dr. Zahari Bin Md Rodzi, whose worthy guidance, and professional attitude are appreciated in completing this technical report. It is a genuine pleasure to express my deep thanks to those who have been there to keep us figured out and resolved in making their way through, cheering us up every time we felt worn out, and encouraging us throughout the study. We are deeply grateful to our parents, who have continuously supported us financially to carry out this study, and for their encouragement and inspiration. Finally, we thank our parents for their moral support throughout this study.

TABLE OF CONTENTS

ABSTRACT

This study proposed mathematical modelling of the RSA cryptosystem based on the modification of modular exponentiation with Hessian curves. Due to the attacker's potential to attack the system, the lack of cryptosystems motivates the study to improve the mathematical modeling of the RSA cryptosystem. If the attackers develop a reverse procedure, the small number of private keys may lead to a lack of resistance against factorization, and the private key 'd' may also be exposed in the decryption phase. The study aims to modify the previous research articles by Dubey and Yadav (2015) from three prime numbers into four prime numbers to compute the composite of n. Besides, the study applied the point addition of Hessian curves in the key generation process and modified the public key e inspired by Intila et al. (2019) based on modular exponentiation in the encryption. The concepts of modular exponentiation, modular inverse and linear congruence were involved in the calculation of the study. Through the study, new mathematical modelling was derived on the key generation, encryption, and decryption process. Then, the numerical example is given with the implementation of the Desmos and Phyton software to test the proposed system. Consequently, the proposed system successfully satisfies the principle of the RSA cryptosystem motivated by Intila et al. (2019) and Dubey and Yadav (2015). Henceforth, all Hessian curve articles inspired by Fouotsa (2019), Smart (2001), and Naveen et al. (2019) are applicable to the proposed mathematical modelling of the RSA cryptosystem. This study can further extend by modifying with some logical developments in mathematical calculation and the Chinese Remainder Theorem to hide many texts into a single plaintext (Intila et al., 2019). Furthermore, this research may extend to develop the mathematical modelling of RSA using large prime numbers and the point doubling of the Hessian curve.