`

UNIVERSITI TEKNOLOGI MARA

TECHNICAL REPORT

MATHEMATICAL MODELLING ON COMMUNICATION BETWEEN TWO PARTIES
(P24M22)

NOR ANEES ASYIQIN BINTI MD DISA
(2020963677)
KHAIRUNNISA MUNAWARAH BINTI KHAIRUL ANWAR
(2020980219)
ANIESA FARHANA BINTI MAZLAN
(2020964027)

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

AUGUST 2022

ACKNOWLEDGEMENTS

We are grateful to Allah S.W.T for giving us the strength to complete this project successfully.

We would like to express my gratitude to our supervisor, Miss Nur Lina Binti Abdullah for the continuous support of our study. Her guidance helped us all the time in writing this study. She has taught us the methodology to carry out this study and to present the study work as clearly as possible. We are grateful for what she has offered us. We would also like to thank her for her empathy and great sense of humour.

We would certainly be remiss to not mention and sincerely thank Professor Madya Dr. Nur Azlina Binti Abd Aziz, our lecturer of this study. Without her help, advice and encouragement, this study would not have happened. She always gives feedback and advice about this study to make sure this study is doing perfectly.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABSTRACT

Elliptic Curve Cryptography (ECC) is a key-based technique for encrypting data. A key pair where the private and public keys is often used by an individual in public key cryptography communication procedures to operate the cryptographic system. A shared key is used to implement communication between two parties using an elliptic curve with the prime p and q. The prime number p is chosen to have a finitely large number of points on the elliptic curve to make the cryptosystem more secure. The current research was carried out determine the mathematical modelling on one way communication between two parties using Kuwakado scheme (2018) method with the proposed system of key exchange on ECC using the operation in generating point. This descriptive-analytical was resolved using the formulation of the study such as point addition, point doubling and double-and-add algorithm. Kuwakado scheme (2018) had be summarized in key generation, encryption, and decryption algorithm. In this study, point $m = (2,4)$ is chosen since it exists on the elliptic curve and will be calculated until 11G using double-and-add algorithm. To test the proposed system of key exchange, the suitably points are important for the receiver including the same and different value of points x on elliptic curve. The proposed method of two-party one-way communication and the ECC key exchange protocol may be extended in future research to explore experimental numerical examples of element selection. The algorithm can be developed by using MAPLE software to generate points and calculate the procedure more easily. Since the key exchange process is successful, we think the offered methods are effective.