UNIVERSITI TEKNOLOGI MARA

TECHNICAL REPORT

APPLICATION OF MELLIN-KAMAL TRANSFORMATION IN EL GAMAL CIPHERTEXT CRYPTOSYSTEM

NURUL SYAZWANI BINTI HUSAIRI –2020834756
NURUL AQILAH BINTI MOHD FAUZI – 2020845016

P30M23

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

AUGUST 2023

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 sincere gratitude to our supervisor, Madam Nur Lina Binti Abdullah, who provided us with an abundance of help and guidance during the 2-semester session of 2022 / 2023. We would also like to thank the lecturers for their collaboration during the completion of the final year project that provided us with useful information, ideas and guidance in compiling and preparing this final year project report.

Last but not least, our deepest appreciation goes out to our parents, family, and others for their cooperation, encouragement, constructive suggestions, and full support for the report's completion. The project would not have been possible without the support of our friends and family, as well as those who contributed to our work and helped us along the way.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABSTRACT

El Gamal ciphertext cryptosystem is one of the fluently used algorithms to satisfy the security message or data transmission. Even though this algorithm alone can satisfy the need of ciphertext cryptosystem, it is vulnerable to numerous internal and external attackers such as logjam and dictionaries attack. So, in order to cover this disadvantage, the modification of El Gamal algorithm with application of Mellin-Kamal transformation was proposed in this study. Our main objective is to compute encryption process and develop decryption schemes using Mellin Transformation and to modify the basic El Gamal system with the application of Mellin-Kamal Transformation. On this proposed scheme, the Mellin transformation is applied on encryption and decryption process and the ciphertext obtained from applied Mellin theorem will then be used as message in Mellin-Kamal cryptosystem. This approach successfully in preventing vulnerable threats and enhance the security through the proposed scheme. Cryptographers often face a problem on key distribution process because of the existent exponential powers and modular multiplication that slower the progress. Other than that, on their proposed scheme, which is Mellin transformation scheme, Bhatti et al. (2020) seem to make the working progress in a rush which result in an uncompleted progression. So, this study contributed to show a complete calculation and working to assist other future researchers know the complete step of the proposed scheme and reduce the probability of middle attackers and strengthen the existing algorithm with several cryptosystem integration. In the further, this study can be applied on asymmetric cryptosystem by taking a large prime number and finite arrangement. Lastly, to recognize the accessibility of the proposed scheme, it can be applied on another existing cryptosystems such as digital signature schemes.

Keywords: Mellin transformation, ElGamal algorithm, Kamal transformation