

UNIVERSITI TEKNOLOGI MARA

TECHNICAL REPORT

**IMPLEMENTATION OF THE MERKLE-HELLMAN
KNAPSACK CRYPTOSYSTEM INTO STATION-TO-STATION
PROTOCOL**

(P09M23)

**NURZHULAIKA BINTI YAHYA (2020834032)
NOOR IZZAH BINTI AGIL (2020489936)
NUR 'AFINI BINTI NORDIN (2020853324)**

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

AUGUST 2023

ACKNOWLEDGEMENTS

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

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 appreciation to all those who helped us complete this study. First, we would like to express our gratitude to our supervisor, Sir Md Nizam Bin Udin who guided, advised, and helped us through this study was conducted. Also, to our lecturer Dr. Zahari bin Md Rodzi (MSP) who has kept us on track every week until this study was a success. Besides, our family and friends who keep supporting us since this study was given. They helped make a big impact to us to keep mentally and physically strong to prepare for this final year project. Not to forget our classmates, housemates and lecturers that always help us by providing motivation, collaboration, and a sense of camaraderie throughout our study.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS	ii
TABLE OF CONTENTS	iii
LIST OF TABLES	iv
LIST OF FIGURES	v
ABSTRACT	vi
CHAPTER 1: INTRODUCTION.....	1
1.1 Motivation.....	1
1.2 Problem Statement.....	4
1.3 Research Question	4
1.4 Objectives	5
1.5 Significant and Benefit of Study.....	5
1.6 Scope and Limitation of Study	6
1.7 Definition of Terms.....	6
CHAPTER 2: BACKGROUND THEORY AND LITERATURE REVIEW	8
2.1 Background Theory	8
2.2 Literature Review and Related Research.....	9
CHAPTER 3: METHODOLOGY AND IMPLEMENTATION.....	14
3.1 Literature Studies	15
3.1.1 Diffie Hellman Key Exchange.....	15
3.1.2 Station-To-Station (STS) Protocol.....	18
3.1.3 Merkle-Hellman knapsack cryptosystem.....	22
3.2 Modification Merkle-Hellman knapsack cryptosystem to be a digital signature	24
3.3 Implementation of Merkle-Hellman digital signature to STS Protocol.....	24
3.4 Development Maple of the proposed method	26
3.5 Comparison table of security level proposed method with previous study	27
CHAPTER 4: RESULT AND DISCUSSION.....	28
4.1 Overview	28
4.2 Implementation Merkle-Hellman knapsack cryptosystem into Station-To-Station Protocol.....	29
4.3 Maplet Interface	35
4.4 Comparison propose method with previous study.....	37
CHAPTER 5: CONCLUSION AND RECOMMENDATION	40
5.1 Conclusion	40
5.2 Recommendation	41
REFERENCES.....	42
APPENDIX	46

LIST OF TABLES

Table 1: Definition of terms and concepts6
Table 2: Comparison of proposed method with previous study37

ABSTRACT

The Merkle-Hellman Knapsack Encryption Cryptosystem is the first widely used public key encryption algorithm. Martin Hellman and Ralph Merkle came up with the idea in 1978. The station-to-station protocol is integrated with the Merkle-Hellman knapsack cryptosystem for a particular use or application when the Merkle-Hellman knapsack cryptosystem is included into the protocol. A cryptographic mechanism called station-to-station is used to provide a secure channel of communication between two parties. Mutual authentication and key exchange for cryptography are involved. Using the Merkle-Hellman knapsack cryptosystem as a part of the station-to-station protocol to improve the protocol's security or effectiveness might be considered integrating the Merkle-Hellman knapsack cryptosystem. The objectives of this study are to modify Merkle-Hellman knapsack cryptosystem to be a digital signature. Then, to implement Merkle-Hellman digital signature into Station-To-Station Protocol. Next, to develop maple for interface the proposed method. Finally, to compare the strength of the security level of the proposed method with the other digital signature. This study aims to demonstrate the implementation of the Merkle-Hellman cryptosystem into the Station-to-Station protocol as a new enhancement. This study also develops maple to show the process of protocol and supported by manual calculation. In conclusion, Station-to-Station securely exchanges keys using Merkle-Hellman knapsack cryptosystem. Despite challenges, the study achieved objectives and validated the system through manual calculations. Comparing articles highlighted superincreasing importance for security. However, errors in sequence creation can compromise it. Modern protocols prefer alternatives like Diffie-Hellman or elliptic curve cryptography. Recommendations for future improvements in the Station-to-Station protocol include implementing a signcryption scheme, combining digital signature and encryption functionalities for enhanced security and cost-efficiency. This approach reduces the operational cost for signature generation and verification. Overall, objectives were successfully met.