MIIEx2017

Melaka International Intellectual Exposition

PROGRAMME ABSTRACT

"Bridging Gaps with Creativity for Future Sustainability"

MIIEx2017

"Bridging the Gaps with Creativity for Future Sustainability"

EDITORS AND COMPILERS:
Prof. Madya Dr. Shafinar Binti Ismail
Mohd Halim Bin Mahphoth
Aemillyawaty Binti Abas
Fazlina Mohd Radzi
Aidah Alias
Ilinadia Jamil
Nor Yus Shahirah Hassan
Shafirah Shaari
Farihan Azahari

COVER DESIGN:
AFTI Sdn Bhd

PUBLISHED BY:
Division of Research and Industry Linkages
Universiti Teknologi MARA MELAKA
KM26 Jalan Lendu,
78000 Alor Gajah Melaka
Tel +606-5582094/ +606-5582190 / +606-5582113
Web: www.miiex2017.com

SHAMIR SECRET SHARING SCHEME USING NEWTON DIVIDED DIFFERENCE INTERPOLATI

Md Nizam Bin Udin, Farah Azliney Amin , Rahmah Shahril,
Naufal Mohd Nasir & Nur Shafiqah Ahmad Bzayauddin

UITM NEGERI SEMBILAN, KAMPUS SEREMBAN

Abstract

Shamir Secret Sharing Scheme proposed by Adi Shamir (1978) is a type of algorithm in cryptography. It is a method to secure the secret by dividing it into several parts so that every participant has its own unique part and when a member or more combine together the secret could be revealed. Rivest, Shamir and Adlemen Algorithm or commonly known as RSA Cryptography proposed in the year 1978 to secure confidential information. Shamir Secret Sharing Scheme was originally developed using Lagrange Interpolation polynomial. The objectives of this research are to apply Newton Divided Difference Interpolation into Shamir Secret Sharing Scheme. Then compare Newton Divided Difference Interpolation with Lagrange Interpolation and validate whether it obtain the same result or vice versa. Newton Divided Difference Interpolation will implement into RSA Cryptography in order to secure the private key. Lastly this project will construct a Graphical User Interface (GUI) using Maple 17. Creating a GUI will enable users to secure confidential information with less time required and more user- friendly. Besides, it is for beginner's cryptography to understand about Shamir Secret Sharing Scheme. The research concludes that Shamir Secret Sharing Scheme also can use Newton Divided Difference Interpolation as their method and not only limited to Lagrange Interpolation. Newton Divided Difference Interpolation also could be implemented in RSA Cryptography and the GUI was successfully created hence archiving what has been stated in objectives.