



PROF. MADYA DR. NUR HAFIZA BINTI ZAKARIA

PENSYARAH UNIVERSITI DS14

CONTACT

Phone: -

E-mail:
mzhafiza@usim.edu.my

Address: Fakulti Sains Dan
Teknologi

SUPERVISION

PhD - Completed: 1, Ongoing: 4

Master - Completed: 0, Ongoing: 0

AREAS OF EXPERTISE

Cryptography

Other Computer Software And Services

Information, Computer And Communication Technologies

BIOGRAPHY

A lecturer from Fakulti Sains Dan Teknologi. Holds a Phd in Security In Computing.

ACADEMIC QUALIFICATION

Phd in Security In Computing (2016)

Master in Science (2012)

Bachelor in Computer Science (2009)

RESEARCH

1. ENHANCING CRYPTOGRAPHIC RESILIENCE THROUGH
SYMMETRIC ENCRYPTION ALGORITHM UTILIZING VARIABLE
LENGTH CHROMOSOMES GENETIC ALGORITHM

2024

ON GOING

MAIN RESEARCHER

2. A NEW DNA-INSPIRED SYMMETRIC ENCRYPTION ALGORITHM FOR
STRONG RANDOMNESS PROPERTIES.

2020

COMPLETED

MAIN RESEARCHER

3. DYNAMIC S-BOX USING AFFINE TRANSFORMATION TO INCREASE
THE SECURITY OF ENCRYPTION

2018

COMPLETED

MAIN RESEARCHER

PUBLICATION

1. SAKTI?: SECURED CHATTING TOOL THROUGH FORWARD SECRECY

2024 JOURNAL

2. DESIGN AND IMPLEMENTATION OF A GENETIC ALGORITHM-BASED BLOCK CIPHER FOR ENHANCED CRYPTOGRAPHIC SECURITY

2024 PROCEEDING

3. REPORT ON THE PHASE 1 EVALUATION OF EXISTING CRYPTOGRAPHIC ALGORITHMS (AKSA) CONSIDERED FOR MYSEAL 2.0 (VERSION 1.2)

2023 POLICY

4. SECURITY ANALYSIS BETWEEN STATIC AND DYNAMIC S-BOXES IN BLOCK CIPHERS

2019 JOURNAL

5. SECURITY ANALYSIS BETWEEN STATIC AND DYNAMIC S-BOXES IN BLOCK CIPHERS

2019 PROCEEDING

6. A BLOCK CIPHER BASED ON GENETIC ALGORITHM

2017 BOOK

7. A BLOCK CIPHER BASED ON GENETIC ALGORITHM

2017 BOOK

8. DESIGNING NEW BLOCK CIPHER BASED ON GENETIC ALGORITHM APPROACH.

2015 JOURNAL

9. ENHANCING ADVANCED ENCRYPTION STANDARD (AES) S-BOX GENERATION USING AFFINE TRANSFORMATION

2015 JOURNAL

10. MODIFIED A5/1 BASED STREAM CIPHER FOR MODIFIED A5/1 BASED STREAM CIPHER FOR MODIFIED A5/1 BASED STREAM CIPHER FOR MODIFIED A5/1 BASED STREAM CIPHER FOR SECURED SECURED SECURED GSM GSM GSM GSM COMMUNICATION COMMUNICATION COMMUNICATION COMMUNICATION

2011 JOURNAL

11. THE SECURITY LEVEL OF TWO XORED-BASED A5 CRYPTO SYSTEM

2011 JOURNAL

12. THE SECURITY LEVEL OF TWO XORED-BASED A5 CRYPTO SYSTEMS

2011 PROCEEDING

CONSULTATION/ADULATION

1. PASUKAN PERUNDING SISTEM E-WALLET (USIMPAY) USIM

2023 UNIVERSITY USIM

2. PANEL PAKAR PENILAI ALGORITMA KRIPTOGRAFI SEDIA ADA (AKSA)

2023 NATIONAL CYBER SECURITY MALAYSIA

3. PROJEK PEMBANGUNAN SENARAI ALGORITMA KRIPTOGRAFI TERPERCAYA NEGARA (MYSEAL)

2017 NATIONAL CYBER SECURITY MALAYSIA

4. Perundingan - Panel Pakar Penilai MySEAL

National Cyber Security Malaysia

AWARDS/RECOGNITION

1. ANUGERAH PENERBITAN JURNAL BERINDEKS WOS/SCOPUS/MYCITE

2025 UNIVERSITY

2. ANUGERAH PENERBITAN PROSIDING BERINDEKS WOS/SCOPUS/MYCITE

2025 UNIVERSITY

3. VISITING SCHOLAR

2025 INTERNATIONAL

4. A HYBRID LLM-GAN AUDIO STEGANOGRAPHY METHOD FOR SECURE MENTAL HEALTH COMMUNICATION

2025 Kebangsaan Gold

5. A CLOUD-BASED HYBRID CERTIFICATE AUTHORITY MODEL INTEGRATING THRESHOLD CRYPTOGRAPHY AND TEMPORAL SHARED KEYS

2025 Antarabangsa Silver