

PROF. MADYA DR. NUR HAFIZA BINTI ZAKARIA

PENSYARAH UNIVERSITI DS14

CONTACT

PHONE

-

E-MAIL

mzhafiza@usim.edu.my

FACULTY

Fakulti Sains Dan Teknologi

SUPERVISION

	COMPLETED	ONGOING
PhD	1	4
Master	0	0

AREAS OF EXPERTISE

- Cryptography
- Other Computer Software And Services
- Information, Computer And Comunication Technologies

ACADEMIC QUALIFICATION

- 2016 **PhD** - Security In Computing
- 2012 **Master** - Science
- 2009 **Bachelor** - Computer Science

RESEARCH

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

2024 | GERAN KPT | ON GOING | MAIN RESEARCHER

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

2020 | GERAN KPT | COMPLETED | MAIN RESEARCHER

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

2018 | GERAN PENYELIDIKAN USIM | COMPLETED | MAIN RESEARCHER

PUBLICATION

1. SAKTI: SECURED CHATTING TOOL THROUGH FORWARD SECRECY

JOURNAL OF ADVANCE RESEARCH IN APPLIED SCIENCES AND ENGINEERING TECHNOLOGY

2024 JOURNAL OTHER DATABASE MAIN AUTHOR

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

SEMINAR ANTARABANGSA ISLAM DAN SAINS (SAIS) 2024

2024 PROCEEDING NON-INDEX MAIN AUTHOR

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

JOURNAL OF INFORMATION SYSTEM AND TECHNOLOGY MANAGEMENT

2019 JOURNAL MYCITE MAIN AUTHOR

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

LANGKAWI INTERNATIONAL MULTIDISCIPLINARY CONFERENCE 2019 (LIMC 2019)

2019 PROCEEDING NON-INDEX MAIN AUTHOR

6. A BLOCK CIPHER BASED ON GENETIC ALGORITHM

2017 BOOK MAIN AUTHOR

7. A BLOCK CIPHER BASED ON GENETIC ALGORITHM

2017 BOOK MAIN AUTHOR

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

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND INFORMATION SECURITY

2015 JOURNAL WOS MAIN AUTHOR

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

JOURNAL OF THEORETICAL AND APPLIED INFORMATION TECHNOLOGY

2015 JOURNAL SCOPUS MAIN AUTHOR

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 SECURED GSM GSM GSM GSM COMMUNICATION COMMUNICATION COMMUNICATION COMMUNICATION

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND NETWORK SECURITY

2011 JOURNAL OTHER DATABASE MAIN AUTHOR

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

INTERNATIONAL CONFERENCE ON RESEARCH AND EDUCATION IN MATHEMATICS (ICREM).

2011 JOURNAL OTHER DATABASE MAIN AUTHOR

PUBLICATION

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

INTERNATIONAL CONFERENCE ON RESEARCH AND EDUCATION IN MATHEMATICS (ICREM).

2011 PROCEEDING NON-INDEX MAIN AUTHOR

CONSULTATION

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

USIM

2023 UNIVERSITY

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

CYBER SECURITY MALAYSIA

2023 NATIONAL

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

CYBER SECURITY MALAYSIA

2017 NATIONAL

4. Perundingan - Panel Pakar Penilai MySEAL

Cyber Security Malaysia

National

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

UNIVERSITAS MUSLIM INDONESIA

2025 INTERNATIONAL

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

Final Year Project & Postgraduate (FYPP): Research & Innovation Poster Competition 2025

2025 KEBANGSAAN GOLD

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

INNOVATION BANK CHALLENGE 2025

2025 ANTARABANGSA SILVER