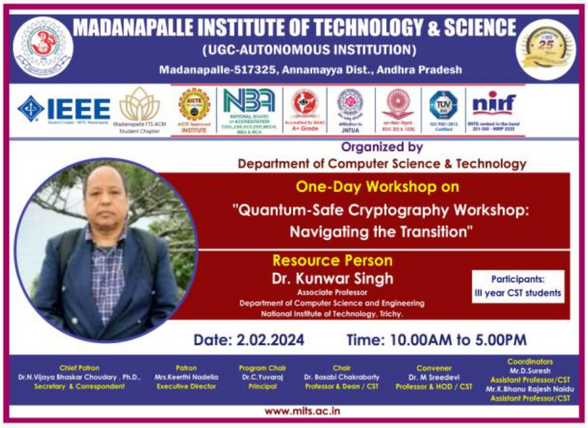
MADANAPALLEINSTITUTEOF TECHNOLOGY &SCIENCE
(UGC-AUTONOMOUS INSTITUTION)
Affiliated to JNTUA, Ananthapuramu &Approved by AICTE, New Delhi
NAAC Accredited with A+ Grade
NBA Accredited -B.Tech. (CIVIL, CSE, ECE, EEE, MECH), MBA & MCA

DEPARTMENT OF COMPUTER SCIENCE & TECHNOLOGY

Report on "One-Day Workshop on Quantum-Safe Cryptography Workshop: Navigating the Transition" On 02.02.2024



MADANAPALLE INSTITUTE OF TECHNOLOGY & SCIENCE
(UGC-AUTONOMOUS INSTITUTION)
Madanapalle-517325, Annamayya Dist., Andhra Pradesh

Organized by
Department of Computer Science & Technology

One-Day Workshop on
"Quantum-Safe Cryptography Workshop:
Navigating the Transition"

Resource Person
Dr. Kunwar Singh
Associate Professor
Department of Computer Science and Engineering
National Institute of Technology, Trichy.

Participants:
III year CST students

Date: 2.02.2024 Time: 10.00AM to 5.00PM

Chief Patron
Dr.N.Vijaya Bhaskar Choudary , Ph.D.,
Secretary & Correspondent

Patron
Mrs.Keerthi Nadella
Executive Director

Program Chair
Dr.C.Yuvaraj
Principal

Chair
Dr. Basabi Chakraborty
Professor & Dean / CST

Convener
Dr. M Sreedevi
Professor & HOD / CST

Coordinators
Mr.D.Suresh
Assistant Professor/CST
Mr.K.Bhanu Rajesh Naidu
Assistant Professor/CST

www.mits.ac.in

Organized by:
1.Mr. D.Suresh, Assistant Professor, Department of CST
2.Mr.K.Bhanu Rajesh Naidu, Assistant Professor, Department of CST

Submitted by:
Mr.K.Bhanu Rajesh Naidu, Assistant Professor, Department of CST

Resource Person Details:
Dr. Kunwar Singh,
Associate Professor,
Department of Computer Science and Engineering,
National Institute of Technology, Trichy.

Participants: III Year CST Students
Attendance: 72 participants
Venue: CST Department,
Mode: Offline

Department of Computer Science & Technology has organized **"One-Day Workshop on Quantum-Safe Cryptography Workshop: Navigating the Transition" on 02.02.2024** (Friday) in Madanapalle Institute of Technology & Science from 10.00 AM to 05:00 PM.

WELCOME ADDRESS

The event commenced promptly at 10:00 AM with a warm and engaging welcome address to all by **Mr.K.Bhanu Rajesh Naidu, Assistant Professor, Department of CST,** Madanapalle Institute of Technology & Science **(**MITS), Madanapalle. The main objective of a **"One-Day Workshop on Quantum-Safe Cryptography Workshop: Navigating the Transition"** Exploring the Post-Quantum Cryptographic Algorithms, Assessing Readiness and Identifying Challenges, Discussing Implementation Strategies, Promoting Collaboration and Knowledge Sharing etc.,

Resource Person Lecture:
Dr.Kunwar Singh, Associate Professor, Department of Computer Science and Engineering, National Institute of Technology, Trichy started to explain about Quantum-Safe Cryptography,

1)Understanding Quantum Computing and Its Implications for Cryptography:

Quantum computing leverages the principles of quantum mechanics to perform computations exponentially faster than classical computers. One of its potential applications is breaking widely used cryptographic algorithms, such as RSA and ECC, by exploiting their vulnerability to quantum algorithms like Shor's algorithm. This understanding is crucial for appreciating the urgency of transitioning to quantum-safe cryptography.

2) Exploring Post-Quantum Cryptographic Algorithms:

Post-quantum cryptography refers to cryptographic algorithms that are believed to be secure against attacks by both classical and quantum computers. Examples include lattice-based cryptography, code-based cryptography, hash-based cryptography, and multivariate polynomial cryptography. Workshop participants can delve into the mathematical foundations and security properties of these algorithms to understand their viability as replacements for current cryptographic standards.

3) **Assessing the Readiness of Current Systems:**

Assessing the readiness of current cryptographic systems involves evaluating their vulnerability to quantum attacks and identifying potential weaknesses. This includes analyzing widely used protocols like TLS/SSL, SSH, and IPsec to determine whether they need to be updated or replaced with quantum-safe alternatives.

4) **Identifying Challenges and Opportunities:**

Transitioning to quantum-safe cryptography presents several challenges, including interoperability with existing systems, standardization of post-quantum algorithms, and managing the transition period. Workshop participants can identify these challenges and explore potential solutions, such as developing migration strategies, establishing industry-wide standards, and fostering collaboration between researchers and practitioners.

5)Discussing Implementation and Deployment Strategies:

Implementing and deploying quantum-safe cryptographic solutions requires careful planning and consideration. Workshop discussions can focus on topics such as integrating post-quantum algorithms into existing software and hardware, ensuring backward compatibility with legacy systems, and educating stakeholders about the importance of transitioning to quantum-safe cryptography.

Resource Person Also Discuss the Topic:

Major Companies Leading the Quantum-Safe Transition

• **AWS's Quantum-Safe Initiatives:** AWS Key Management Service (KMS) supports post-quantum hybrid key exchange for transport layer security (TLS), blending classical and quantum-resistant schemes to mitigate future decryption risks.

• **Microsoft's Quantum-Safe Program:** Microsoft is actively working towards quantum safety across its products, adhering to existing symmetric key encryption and hash function algorithms and prioritizing PQC algorithms.

• **Google's Quantum-Resistant Implementations:** Google's FIDO2 security key, which combines ECC security with the quantum-resistant algorithm Dilithium, is part of its broader strategy for adopting quantum-resistant cryptographic algorithms.

Vote of thanks

The guest lecture formally concluded with a vote of thanks delivered by **Mr. D. Suresh, Assistant Professor**, **Department of CST**. In his address, he expressed sincere gratitude to resource person for taking the time to share his expertise and inspire our students.

Outcomes:

At the end of Program, Students can able to,

1. Explore basics of quantum computing and its implications for cryptography.
2. Explore Post-Quantum Cryptographic Algorithms.
3. Identify challenges such as interoperability issues, standardization concerns, and performance considerations associated with transitioning to quantum-safe cryptography.
4. Implement strategies for deploying quantum-safe cryptographic solutions.
5. Articulate the tools and resources needed to navigate the transition to quantum-safe cryptography effectively.