1. **Name and Full Correspondence Address** : Dr. Vandana
   Assistant Professor
   Department of Applied Sciences and Humanities (DASH)
   NIAMT Hatia
   Ranchi-834003
2. **Email(s) and contact number(s)** : vandana.math@gmail.com
   +91-9955215816
3. **Institution** : National Institute of Advanced Manufacturing Technology Hatia, Ranchi, Jharkhand-834003
4. **Gender (M/F/T)** : F
5. **Category Gen/SC/ST/OBC** : Gen (UR)
6. **Whether differently abled (Yes/No)** : No

ACADEMIC QUALIFICATIONS (UNDERGRADUATE ONWARDS):

1. **B.Sc. (in 2004) -** In Non-Medical, from SMDRSD College Pathankot, 76.75%
2. **M.Sc. (in 2006) -** In Mathematics, from Guru Nanak dev University Campus, Amritsar, 86.3%
3. **M.Phil. (in 2008) -** In Mathematics, from Himachal Pradesh University Shimla, 81%
4. **MTech. (in 2011) -** In Computer Application, from Indian Institute of Technology Delhi, CGPA 9.1
5. **Ph.D. (in 2015) -** In Cryptography, from Indian Institute of Technology Kharagpur, CGPA 9.2

Ph.D. THESIS TITLE, GUIDE'S NAME, INSTITUTE/ORGANIZATION/UNIVERSITY, YEAR OF AWARD:

Thesis Title	:	Designs of Universally Composable Secure Adaptive Oblivious Transfer Protocols
Research Area	:	Cryptography (Mathematics)
Guide's Name	:	Dr. Ratna Dutta
Institute	:	Department of Mathematics Indian Institute of Technology Kharagpur
Years Active	:	July 2011 -- June 2015
Year of Award	:	2015

WORK EXPERIENCE (IN CHRONOLOGICAL ORDER):

1. Assistant Professor at National Institute of Advanced Manufacturing Technology Hatia, Ranchi; joined on 21/12/2023
2. Assistant Professor at Birla Institute of Technology Mesra; from 23/05/2017 to 20/12/2023
3. Post Doctoral Fellow at Indian Institute of Technology Kharagpur; from 8/7/2016 to 22/5/2017

PROFESSIONAL RECOGNITION/ AWARD PRIZE/ CERTIFICATE, FELLOWSHIP RECEIVED BY THE APPLICANT:

1. Gold Medal from GNDU Amritsar in 2006
2. Gold Medal from HPU Shimla in 2008
3. Gold Medal from IIT Delhi in 2011
4. M.Tech. Fellowship from CSIR in 2009-11
5. Ph.D. Fellowship from IIT Kharagpur in 2011-15
6. Post-Doctoral Fellowship from NBHM in 2016-17

PG. STUDENT SUPERVISION:

1. In 2023; Apurva; Roll- IMH/10044/2018; Project Work.
2. In 2023; Chayanika Goswami; Roll- IMH/10060/2018; Project Work.
3. In 2023; Ranjeet Kumar; Roll- IMH/10069/2018; Project Work.
4. In 2023; Ravi Shankar Jha; Roll- IMH/10076/2018; Project Work.
5. In 2023; Lakshmi Dathan; SAM/10002/2021; Project Work.
6. In 2023; Riya Agarwal; Roll- IMH/10006/2018; Internship; Company - Floxus
7. In 2023; Shreya Rani; Roll- IMH/10007/2018; Internship; Company - Bulkpe & Floxus
8. In 2023; Pandarinath Gunda; Roll- IMH/10010/2018; Internship; Company - University of Adgar
9. In 2023; Rahul Kumar Patro; Roll- IMH/10012/2018; Internship; Company - Truminds
10. In 2023; Nisha Rani; Roll- IMH/10033/2018; Internship; Company – Navi

11. In 2023; Arjita Basu; Roll- IMH/10051/2018; Internship; Company - Deloitte
12. In 2023; Soumyajit Behera; Roll- IMH/10052/2018; Internship; Company - Juspay
13. In 2023; Anant Anand; Roll- IMH/10063/2018; Internship; Company - Almabetter
14. In 2023; Prateek Agarwal; Roll- IMH/10065/2018; Internship; Company - Almabetter
15. In 2023; Antara Basu; Roll- IMH/10068/2018; Internship; Company - Almabetter
16. In 2022; Ashish Pandey; Roll- IMH/10072/2017; Internship Project; Topic- Learning technologies like Java, Python, CSS3, HTML, and JavaScript.
17. In 2022; Asmita Kumari; Roll- IMH/10015/2017; Thesis; Topic- Implementation of Image Encryption and Decryption using RSA algorithm
18. In 2022; Shiny Chakraborty; Roll- IMH/10065/2017; Thesis; Topic- On an Image Encryption Methodology using Elliptic Curve Cryptography with Hill Cypher
19. In 2022; Neeharika Senapati; Roll- IMH/10016/2017; Thesis; Topic- Implementation of Image Encryption and Decryption using AES algorithm
20. In 2022; Sibasish Padhy; Roll- IMH/10023/2017; Thesis; Topic- Implementation of Deep Learning Techniques in Demand Planning
21. In 2022; Kaushal Kumar Mishra; Roll- IMH/10080/2017; Thesis; Topic- Self-Driving AI Car Application
22. In 2022; Harsimran Kaur; Roll- IMH/10039/2017; Thesis; Topic- iOS App Development using Swift
23. In 2021; Aman Kumar Singh; Roll- IMH/10012/2016; Thesis; Topic- Making Scalable Web Apps with Aws and Serverless Technology
24. In 2021; Shubhangi Sinha; Roll- IMH/10008/2016; Thesis; Topic- Making Scalable Web Apps with Aws and Serverless Technology
25. In 2021; Suravi Mishra; Roll- IMH/10024/2016; Thesis; Topic- Making Scalable Web Apps with Aws and Serverless Technology
26. In 2021; Snehil Kishore; Roll- IMH/10005/2016; Thesis; Topic- Making Scalable Web Apps with Aws and Serverless Technology
27. In 2021; Harsh Vardhan Kumar; Roll- IMH/10070/2016; Thesis; Topic- Making Scalable Web Apps with Aws and Serverless Technology
28. In 2021; Yashi Shukla; Roll- IMH/10010/2016; Thesis; Topic- Making Scalable Web Apps with Aws and Serverless Technology
29. In 2019; Rudravajhula Sandhya; Roll- IMH/10002/2014; Thesis; Topic- Application of Dynamic Optimization of a Business Process Technique to the Workflow of Business Units at T-Hub
30. In 2019; Ajay Agalcha; Roll- IMH/10026/2014; Thesis; Topic- Analysis of Color Image Data using Public Key Cryptosystem Associated with 2D-DWT
31. In 2019; Badal Raj; Roll- IMH/10022/2014; Thesis; Topic- Automation of Finance Process Using Blue Prism
32. In 2019; Sakshee Monal; Roll- IMH/100/14; Thesis; Topic- Development of Chatbot for 1530 Restaurants using Amazon Web Services

33. In 2018; Nidhi Jawandhia; Roll- IMH/100/13; Thesis; Topic- Atkin's ECPP (Elliptic Curve Primality Proving) Algorithm
34. In 2018; Kumar Abhishek Anand; Roll- IMH/10019/2013; Thesis; Topic- Cryptography using Artificial Neural Networks
35. In 2018; Pawan Kumar; Roll- IMH/10005/2013; Thesis; Topic- Blockchains and the Mathematics behind it

PUBLICATIONS (LIST OF PAPERS PUBLISHED IN SCI JOURNALS, IN YEAR-WISE DESCENDING ORDER):

1. **Vandana Guleria,** Yashavant Kumar and D. C. Mishra: Multiple colour image encryption using multiple parameter FrDCT, 3D Arnold transform and RSA, Multimedia Tools and Applications, 2023 (Accepted, SCIE)

2. Yashavant Kumar, **Vandana Guleria:** Mixed-multiple image encryption algorithm using RSA cryptosystem with fractional discrete cosine transform and 2D-Arnold Transform, Multimedia Tools and Applications, 2023 (Accepted, SCIE)

3. Shazia Sabir, **Vandana Guleria** : Multi-layer permutation-substution operations based on novel lossless multiple color image encryption, Multimedia Tools and Applications, 2023 (Accepted, SCIE)

4. Shazia Sabir, **Vandana Guleria** : A novel multi-layer color image encryption based on RSA cryptosystem, RP2DFrHT and generalized 2D Arnold map, Multimedia Tools and Applications, 82, 38509–38560, 2023 (SCIE)

5. Shazia Sabir, **Vandana Guleria** : Multi-layer security based multiple image encryption technique, Computers and Electrical Engineering, 106, 108609, 2023 (SCIE)

6. Shazia Sabir, **Vandana Guleria** and D. C. Mishra: Security of multiple RGB images in the time domain and frequency domain, *Journal of Information Security and Applications*, 63, 103005, 2021 (SCIE)

7. Shazia Sabir, **Vandana Guleria**: Multi-layer color image encryption using random matrix affine cipher, RP2DFrHT and 2D Arnold map, Multimedia Tools and Applications, 80(18), 27829—27853, 2021 (SCIE)

8. **Vandana Guleria**, DC Mishra: Multiple RGB image encryption algorithm with multilayers by Affine Hill Cipher with FrDCT and Arnold Transform, Fractals, 29(16), 2150151, 2021. (SCIE)

9. **V. Guleria** and D.C. Mishra: New multi-layer RGB image encryption algorithm based on Diffie-Hellman cryptography associated with FrDCT and Arnold Transform, *Multimedia Tools and Applications*, 79(43), 2020, 33119--33160 (SCIE)

10. Anand Joshi, Dhanesh Kumar, D.C. Mishra, and **V. Guleria**: Color-image encryption based on 2D discrete wavelet transform and 3D logistic chaotic map, J*ournal of Modern Optics*, 67(10), 2020, 933--949 (SCI)

11. **V. Guleria,** Shazia Sabir, and D.C. Mishra: Security of Multiple RGB Images by RSA Cryptosystem Combined with FrDCT and Arnold , Transform, *Journal of Information Security and Applications*, 54, 2020, 102524 (SCIE)

12. R. Singh, **V. Guleria,** M. Singh: Haar wavelet quasilinearization method for numerical solution of Emden-Fowler type equations, *Mathematics and Computers in Simulation*, 174, (2020), 123--133. (SCI)

13. J. Srinivas, D. Mishra, S. Mukhopadhyay, S. Kumari, and **V. Guleria.**: An Authentication framework for roaming service in global mobility networks, *Information Technology and Control*, 48(1), (2019), 129-145. (SCIE)

14. R. Singh, H. Garg, and **V. Guleria**.: Haar wavelet collocation method for Lane-Emden equations with Dirichlet, Neumann and Neumann-Robin boundary conditions, *Journal of Computation and Applied Mathematics*, 340, 150-161 (2019). (SCI)

15. **V. Guleria** and R. Dutta.: Efficient Oblivious Transfer with Adaptive Queries in UC Framework, *Security and Communication Networks*, 9(15), 2592-2611 (2016). (Wiley, SCIE)

16. **V. Guleria** and R. Dutta.: Universally Composable Issuer-Free Adaptive Oblivious Transfer with Access Policy, Security and Communication Networks, 8(18), 3615-3633 (2015). (Wiley, SCIE)

PUBLICATIONS (LIST OF PAPERS PUBLISHED IN INTERNATIONAL CONFERENCE PROCEEDINGS LNCS, SPRINGER-VERLAG), IN YEAR-WISE DESCENDING ORDER):

1. **V. Guleria** and R. Dutta.: Efficient Adaptive Oblivious Transfer in UC Framework. ***In the Proceeding of the 10th Information Security Practice and Experience Conference (ISPEC 2014)***, LNCS, vol. 8434, pp. 271--286, Springer-Verlag.
2. **V. Guleria** and R. Dutta.: Lightweight Universally Composable Adaptive Oblivious Transfer. ***In the Proceeding of the 8th International Conference on Network and System Security (NSS 2014)***, LNCS, vol. 8792, pp. 285--298, Springer-Verlag.
3. **V. Guleria** and R. Dutta.: Adaptive Oblivious Transfer with Hidden Access Policy Realizing Disjunction. ***In the Proceeding of the 11th International Conference on Security and Cryptography (SECRYPT 2014),*** pp. 43--54.
4. **V. Guleria** and R. Dutta.: Issuer-Free Adaptive Oblivious Transfer with Access Policy. ***In the Proceeding of the 17th International Conference on Information Security and Cryptology (ICISC 2014),*** LNCS, vol. 8949, pp. 402--418, Springer-Verlag.

5. **V. Guleria** and R. Dutta.: Universally Composable Identity Based Adaptive Oblivious Transfer with Access Control. ***In the Proceeding of the 10th International Conference on Information Security and Cryptology (INSCRYPT 2014),*** LNCS, vol. 8957, pp. 109--129, Springer-Verlag.
6. **V. Guleria** and R. Dutta.: Efficient Adaptive Oblivious Transfer without q-type Assumptions in UC Framework. ***In the Proceeding of the 16th International Conference on Information and Communications Security (ICICS 2014),*** LNCS, vol. 8958, pp. 105--119, Springer-Verlag.

Book Chapter:

1. **V. Guleria** and R. Dutta.: Adaptive Oblivious Transfer Realizing Expressive Hidden Access Policy. ***E-Business and Telecommunications (ICETE 2014),*** vol. 554, pp. 212--233, Springer-Verlag.

Electronic Edition @arxiv.org:

1. **V. Guleria** and R. Dutta.: UC Secure Issuer-Free Adaptive Oblivious Transfer with Hidden Access Policy. CoRRabs/1711.10751 (2017

EXTRACURRICULAR ACTIVITIES:

1. ERP Coordinator, Mathematics Department, BIT Mesra, Ranchi, Since January 2021 to 20/12/2023.

AWARDS/DISTINCTIONS:

1. Secured 5th in Guru Nanak Dev University in B.Sc.
2. Secured 13th position in State Board (PSEB) in +2.
3. Merit Holder in 10th.

QUALIFIED EXAMINATIONS:

1. Qualified (Gate) Graduate Aptitude Test in Engineering (2009-AIR-2)
2. Qualified CSIR-UGC National Eligibility Test (JRF-June-2009)
3. Qualified CSIR-UGC National Eligibility Test (JRF-December-2008)
4. Qualified CSIR-UGC National Eligibility Test (JRF-June-2008)

TECHNICAL SKILLS:

1. Operating Systems- Windows, Linux

2. Applications- Latex, MS Office
3. Programming Languages- C, MATLAB

CONFERENCES ATTENDED:

1. Presented paper at the 17th International Conference on Information Security and Cryptology (ICISC 2014) held in Seoul, Korea, December 3-5, 2014.
2. Attended the 13th International Conference on Cryptology (INDOCRYPT 2012), held in Kolkata, India, December 9-12, 2012.

WORKSHOPS/SHORT-TERM COURSES ATTENDED:

1. Attended a Short-Term Course on Cryptography, held in Kharagpur, India, May 18-24, 2014.
2. Lectured on Homomorphic Encryption in Short Term Course on Cryptography, held in Kharagpur, India, May 18-24, 2014.
3. Presented a paper on Research Scholar day held in the Department of Mathematics, IIT Kharagpur, India, February 21-22, 2014.
4. Participated in International Conference on Recent Advances in Lattice Reduction Algorithms and their Applications, held in Hyderabad, India, April 10-12, 2012.

ORIENTATION PROGRAMME:

1. Attended the 93rd orientation program held at Ranchi University, 20/11/2018-17/12/2018.

DECLARATION:

I hereby declare that the information furnished above is accurate to the best of my knowledge and belief.

Vandana
Assistant Professor
DASH (Mathematics)
NIAMT Hatia
Ranchi
Jharkhand-834003