Dr. J K M Sadique Uz Zaman
Assistant Professor

Department of Computer Science and Application
University of North Bengal
Raja Rammohunpur, P.O. NBU
Dist. Darjeeling, PIN – 734013
West Bengal, India
Phone: +91 – (0353) 277 6344 (O), 9830960738 (M)
Email: jkmsadique@nbu.ac.in and jkmwbes@gmail.com

Areas of Research Interest: Cryptography, Message Security, Pseudorandom Number Generator (PRNG), Blockchain.

Subject Specialization: Cryptography, DBMS, Algorithms.

Ph.D Thesis Supervised: Completed: 0 Thesis Submitted: 0 Ongoing: 2

Educational Qualification:

Ph.D. (Tech.)	University of Calcutta	Field of research: Cryptography
M.Tech	University of Calcutta	Computer Science and Application
MCA	T.M. Bhagalpur University	Final Project was executed at University of Calcutta
M.Sc.	T.M. Bhagalpur University	Physics

- Qualified the GATE 2012 Examination in Computer Science & Information Technology.
- Qualified the UGC NET Dec-2012 for Lectureship in Computer Science and Applications.

Professional Experience: Junior Programmer, Semaphore Computers Pvt. Ltd., Kolkata – 700012, Platform: Visual Basic, From 01/02/2006 to 04/08/2006.

Scholarship/Fellowship:

1. National Scholarship for class VIII to X.
2. MHRD: National Scholarship, Govt. of India, Secured 52 rank in Madhyamik Pariksha, W.B.
3. UGC: UPE Project fellow in Science & Technology, University of Calcutta.
4. UGC: Junior Fellow in RFSMS, University of Calcutta.
5. UGC: JRF in Engineering & Technology, University of Calcutta.
6. UGC: SRF in Engineering & Technology, University of Calcutta.
7. DST: SRF in DST-PURSE Programme, University of Calcutta.

Major/Minor Project:

1. Studies on Public Key Cryptosystems to achieve Better Security in Data Communication, University of North Bengal, 1,50,000/-, Principal Investigator, (Minor Project).

Teaching Experience: 8+ Years

1. Guest Lecturer, Department of Computer Science and Engineering, Aliah University, Kolkata, India, from July 2013 to December 2014.
2. Assistant Professor, Department of Computer Science, APC Roy Govt. College, Siliguri, India, from 18/02/2015 to 19/12/2018.
3. Assistant Professor, Department of Computer Science and Application, University of North Bengal, Siliguri, India, from 20/12/2018 to present.

Member of Professional Body:

1. CRSI (Cryptology Research Society of India): Life Member
2. Library of Indian Statistical Institute, Kolkata: Life Member

Member of Committee:

1. Member, BoS in Computer Science, University of Gour Banga, Malda.
2. Member, Moderation board in Computer Science, University of Gour Banga, Malda.
3. Member, BoS in BCA and B.Sc. Computer Science, University of North Bengal.
4. Member, BoS in M.Sc. Computer Science, University of North Bengal.
5. Member, BoS in MCA, University of North Bengal.
6. Member, DRC, Computer Science and Application, University of North Bengal.
7. Member, Organizing Committee, International Webinar on Emerging Trends in Computational Technologies (IWETCT), Deptt. of CSA, NBU, October 01–03, 2021.
8. <u>Posts hold at A.P.C. Roy Govt. College, Siliguri:</u>
   (i) Website management Sub-committee:
      (a) Joint Convenor from 01/07/2015 to 30/06/2017.
      (b) Member from 01/07/2017 to 30/06/2018.
   (ii) AISHE (All India Survey of Higher Education) Sub-committee:
      (a) Member from 01/07/2015 to 30/06/2016.
      (b) Joint Convenor from 01/07/2016 to 30/06/2017.
      (c) Convenor from 01/07/2017 to 30/06/2018.
   (iii) WBHS Sub-committee:
      (a) Member from 01/07/2015 to 30/06/2016.
      (b) Joint Convenor from 01/07/2016 to 30/06/2017.
      (c) Convenor from 01/07/2017 to 30/06/2018.
   (iv) E-Billing Sub-committee:
      (a) Member from 01/07/2015 to 30/06/2016.
      (b) Joint Convenor from 01/07/2016 to 30/06/2018.
      (c) Member from 01/07/2018 to 19/12/2018.
   (v) Admission Sub-committee:
      (a) Member from 01/07/2015 to 30/06/2017.
      (b) Joint Convenor from 01/07/2017 to 30/06/2018.
      (c) Convenor from 01/07/2018 to 19/12/2018.
   (vi) Apart from these, also performed as a Member of various Sub-committees like Income Tax, Students Election, Student Grievance Cell etc.

Administrative Activity and Other Responsibility:

1. A.P.C. Roy Govt. College Study Centre (K-08) of Netaji Subhas Open University:
   (a) Assistant Coordinator from 15/07/2016 to 18/12/2018.
   (b) Examination Centre-in-Charge, UG-PG examinations, from 02/07/2017 - 03/09/2017.
2. In-Charge of the College in absence of the Officer-In-Charge, A.P.C. Roy Govt. College, Siliguri on 19/08/2016 and 27/06/2018.
3. District Level Student-Youth Science Fair 2019, Govt. of West Bengal: Performed the duty as a Judge of Darjeeling district on 01/10/2019.

Invited Talk:

1. An overview of Cryptology and use of Modular arithmetic in modern Cryptography, One-Day Seminar on Cloud Computing & Cryptography, Jointly Organized by: Techno India College of Technology, New Town, Kolkata and IEEE GOLD, 29th April, 2014.

Professional Development Programme Attended:

1. Orientation Programme (30th OP-NBU) during 01/06/2017 to 28/06/2017 at UGC-HRDC, University of North Bengal, Siliguri, India.
2. Refresher Course (Specific) in Computer Science during 04/01/2019 to 24/01/2019 at UGC-HRDC, University of North Bengal, Siliguri, India.

Publications: 16, Journals – 08, Conference Proceedings and Book Chapters – 08.

Paper Published/Accepted in Journal:

1. Review on fifteen Statistical Tests proposed by NIST, Journal of Theoretical Physics & Cryptography, ISSN: 2322-3138, Vol. 1, 2012, pp. 18-31, **J K M S Zaman** and R.Ghosh.
2. PRNG based Symmetric Stream Cipher, Int. J. Advanced Networking and Applications, ISSN: 0975-0290, Vol. 4(5), 2013, pp. 1725-1730, **J K M S Zaman.**
3. Search for Secure Random 8-bit Generator by Modular Approach of Statistical Test, Int. J. Computer Applications, ISSN: 0975-8887, Vol. 96(10), 2014, pp. 32-41, **J K M S Zaman** and R.Ghosh.
4. A Modular approach on Statistical Randomness Study of bit sequences, Int. J. Advanced Networking and Applications, ISSN: 0975-0290, Vol. 6(1), 2014, pp. 2141-2150, **J K M S Zaman**, S.Saha and R.Ghosh.
5. An Algorithm to find the Irreducible Polynomials over Galois Field GF(p^m), Int. J. Computer Applications, ISSN: 0975-8887, Vol. 109(15), 2015, pp. 24-29, **J K M S Zaman**, S.Dey and R.Ghosh.
6. Study of Randomness in AES Ciphertexts Produced by Randomly Generated S-Boxes and S-Boxes with Various Modulus and Additive Constant Polynomials, J. The Institution of Engineers (India): Series B, ISSN: 2250-2106, Vol. 97(2), 2016, pp. 193–208, Suman Das, **J K M S Zaman** and R.Ghosh.
7. A Pseudorandom Number Generator using Irreducible Polynomial over GF(7^3), Journal of Theoretical Physics and Cryptography, ISSN: 2322-3138, Vol. 12, 2016, pp. 18-25, **J K M S Zaman** and R.Ghosh.
8. Randomized DES Using Irreducible Polynomial Over Galois Field GF(7^3), Int. J. Advanced Research in Computer Science, ISSN: 0976-5697, Vol. 8(7), 2017, pp. 760-766, **J K M S Zaman** and R.Ghosh.

Published/Accepted Book Chapter:

1. Multiplicative Polynomial Inverse over GF(7^3): Crisis of EEA and its Solution, **Springer** India 2015, Applied Computation and Security Systems, Advances in Intelligent Systems and Computing, Vol. 305, pp. 87-107, **J K M S Zaman** and R.Ghosh.
2. Dynamic Ciphering-15 Based on Multiplicative Polynomial Inverses Over Galois Field GF(7^3), **Springer** India 2016, Advanced Computing and Systems for Security, Advances in Intelligent Systems and Computing, Vol. 395, pp. 31-48, **J K M S Zaman**, S.Dey and R.Ghosh.

Paper Published/Accepted in National/International Conference, Seminar, Workshop:

1. Symmetric Block Ciphers using Random S-boxes Dependent on a long key, Jan. 3-7, 2009: Indian Science Congress, Section: Information and Communication Science & Technology (including Computer Sciences), held at NEHU, Shillong, Meghalaya, Abstract published in proceeding, p. 23, authors: **J K M S Zaman** and R.Ghosh.
2. A 4-Character Stream Ciphering Technique by Random Key Substitution: A Concept of Hardware Implementation, Aug.7-9, 2009: National Workshop on Cryptology, held at SVNIT, Surat, Gujarat, jointly organized by CRSI and SVNIT, pp. 42-46, authors: J.Dutta, S.Karmakar, B.Patra, **J K M S Zaman** and R.Ghosh.
3. A Review Study of NIST Statistical Test Suite: Development of an indigenous Computer Package, Sep.23-24, 2011: National Workshop on Cryptology, held at NIIT University, Neemrana, Rajasthan, jointly organized by CRSI and NIIT University, authors: **J K M S Zaman** and R.Ghosh.
4. A Simple 1-byte 1-clock RC4 hardware design and its implementation in FPGA coprocessor for secured Ethernet communication, Aug.6-8, 2012: National Workshop on Cryptology, held at VIT University, Vellore, Tamil Nadu, jointly organized by CRSI and VIT University, pp. 61-70, authors: R.Paul, S.Saha, **J K M S Zaman**, S.Das, A.Chakrabarti and R.Ghosh.
5. Generation of AES S-Boxes with various modulus and additive constant polynomials and testing their randomization, Sep.27-28, 2013: Int. Conference on Computational Intelligence: Modeling Techniques and Applications (CIMTA) 2013, held at Kalyani University, Kalyani, West Bengal, organized by Kalyani University, published in Elsevier, Procedia Technology 10 (2013) 957 – 962, authors: S. Das, **J K M S Zaman** and R. Ghosh.
6. Statistical Randomness Study Based on Three Test Modules with NIST as the One, Oct.3-5, 2013: National Workshop on Cryptology, held at Delhi University, North Campus, New Delhi, organized by Scientific Analysis Group – DRDO under the aegis of CRSI, pp. 1-10, authors: **J K M S Zaman**, S.Saha and R.Ghosh.
7. Multiplicative Polynomial Inverse over GF(7^3): Crisis of EEA and its Solution, Apr.18-20, 2014: Int. Doctoral Symposium on Applied Computation and Security Systems (ACSS 2014), held at CU, Kolkata, jointly organized by University of Calcutta and AGH University of Science and Technology (Poland), authors: **J K M S Zaman** and R.Ghosh. [Published as a book chapter mentioned in (1) above]
8. Dynamic Ciphering-15 Based on Multiplicative Polynomial Inverses Over Galois Field GF(7^3), May.23-25, 2015: Int. Doctoral Symposium on Applied Computation and Security Systems (ACSS 2015), held at CU, Kolkata, jointly organized by University of Calcutta and AGH University of Science and Technology (Poland), authors: **J K M S Zaman** and R.Ghosh. [Published as a book chapter mentioned in (2) above]

Conference, Seminar, Webinar, Workshop Attended:

1. 9th Int. Conference on Cryptology in India, INDOCRYPT 2008, IIT Kharagpur, Dec. 14-17, 2008.
2. CRSI-IMSc Workshop on Teaching Cryptology at Undergraduate Level, held at Applied Statistics Unit, Indian Statistical Institute, Kolkata – 700108, June 15-19, 2009.
3. Pre-Conference Tutorial of the 10th Int. Conference on Cryptology in India, INDOCRYPT 2009, New Delhi, Dec. 13, 2009.
4. 10th Int. Conference on Cryptology in India, INDOCRYPT 2009, New Delhi, Dec. 14-16, 2009.
5. 2-day Tutorial Workshop on Cryptology, Organized by: University of Calcutta and ISI-Kolkata, held at University College of Science and Technology, CU, July 16-17, 2011.
6. Workshop on Embedded System Design: Recent Trends and Techniques, Organized by: A.K.C.S.I.T of Calcutta University and Pracsol Technologies India, Sponsored by TEQIP Phase-II, March 08-10, 2013.
7. One Day Workshop on IoT Analytics & Mobile Crowd Sensing, Department of Computer Science, University of Gour Banga, Malda, West Bengal, March 29, 2019.
8. Cyber Shikshak – a Cyber Security Awareness Training Programme, Organised by Cyber Security Centre of Excellence, Deptt. of IT & Electronics, Govt. of W.B. in collaboration with Indian School of Ethical Hacking (ISOEH), held at Webel IT Park – II, Siliguri, March 17, 2021.
9. International Webinar on Emerging Trends in Computational Technologies (IWETCT), Department of Computer Science and Application, NBU, October 01–03, 2021.

Place: Siliguri
Date: 17/02/2022

J K M Sadique Uz Zaman
[Signature]