

Introduction to Information Security (Half Course: 2 Credits)

Dr. Ashok Kumar Das

IEEE Senior Member
Associate Professor

Center for Security, Theory and Algorithmic Research
International Institute of Information Technology, Hyderabad

E-mail: *ashok.das@iiit.ac.in*

Homepage: <http://www.iiit.ac.in/people/faculty/ashokkdas>

Personal Homepage: <https://sites.google.com/view/iitkgpkdas/>

Welcome to Introduction to Information Security

- **Education:** Ph.D. in Computer Science and Engineering, M.Tech. in Computer Science and M.Sc. in Mathematics (with specialization in Computer Science) from *Indian Institute of Technology, Kharagpur (IIT Kharagpur)*, India
- **Research Interests:** Cryptography, system and network security, blockchain, security in Internet of Things (IoT), Internet of Vehicles (IoV), Internet of Drones (IoD), smart grids, smart city, cloud/fog computing and industrial wireless sensor networks, intrusion detection, AI/ML security
- **Research Highlights [Research Publications (Total: 292)]:**
 - ▶ Number of Journal Papers: 331
 - ▶ Number of Conference Papers: 36
 - ▶ Number of Book Chapters: 9
 - ▶ Number of Edited Books/Volumes: 2
 - ▶ Number of IEEE Transactions/IEEE Journal/IEEE Magazine Papers: 113

- **Total citations: 15,067, h-index: 73, i10-index: 207**
(According to Google Scholar Citations as on January 8, 2023)
- **Published in top venues like**
 - * IEEE Transactions on Information Forensics and Security
 - * IEEE Transactions on Dependable and Secure Computing
 - * IEEE Transactions on Consumer Electronics
 - * IEEE Transactions on Smart Grid
 - * IEEE Transactions on Industrial Informatics
 - * IEEE Transactions on Vehicular Technology
 - * IEEE Internet of Things Journal
 - * IEEE Consumer Electronics Magazine
 - * IEEE Communications Magazine
 - * IEEE Journal of Biomedical and Health Informatics
(Formerly, IEEE Transactions on Information Technology in Biomedicine)
 - * IEEE Transactions on Network Science and Engineering
 - * IEEE Transactions on Intelligent Transportation Systems
 - * IEEE Sensors Journal

About me: Journal Editorial Board Members

- Associate Editor: **IEEE Systems Journal** (SCI Impact Factor: 3.987) [Duration: August 2020 onwards]
- Editor: **Journal of Network and Computer Applications (Elsevier)** (SCI Impact Factor: 5.570) [Duration: October 2020 onwards]
- Editor (Technical Committee): **Computer Communications (Elsevier)** journal (SCI Impact Factor: 2.816) [Duration: August 2020 onwards]
- Associate Editor: **Journal of Cloud Computing (Springer)** (SCI Impact Factor: 5.71) [Duration: August 2021 onwards]
- Associate Editor: **IET Communications** journal (SCI Impact Factor: 1.443) [Duration: February 2019 - February 2022]
- Associate Editor: **Cyber Security and Applications (Elsevier)** [Duration: September 2021 onwards]
- Editor: **KSII Transactions on Internet and Information Systems** (SCI Indexed Journal) (2016 -)
- Editor: **International Journal of Internet Technology and Secured Transactions (Inderscience)** (2016 -)
- Guest Editor: **Computers & Electrical Engineering (Elsevier)** (SCI Indexed Journal), Special issue on Big data and IoT in e-healthcare, 2016
- Guest Editor: **ICT Express (Elsevier)** (ESCI Indexed Journal), Special Issue on Blockchain Technologies and Applications for 5G Enabled IoT, 2019
- Guest Editor: **Wireless Communications and Mobile Computing** (SCI Indexed Journal), Special issue on "Security and Privacy for Smart Mobile Devices: Attacks, Challenges, and New Designs" 2020

- Listed in the **Web of Science (Clarivate™) Highly Cited Researcher 2022** in recognition of exceptional research performance demonstrated by production of multiple highly cited papers that rank in the top 1% for field and year.
- Media coverage on “**China way ahead in blockchain, India needs to catch up**” in the **Times of India newspaper on 6 May 2021** (please see at:
<https://timesofindia.indiatimes.com/business/india-business/china-way-ahead-in-blockchain-india-needs-to-catch-up/articleshow/82428430.cms>)
- Included in the **Stanford University's Top 2% Most Influential Scientists List with Subject Rank (World): 179 for the year: 2021**.
The ranking is based on an independent study done by the Stanford University, USA. For detailed information, please visit:
<https://elsevier.digitalcommonsdata.com/datasets/btchxktzyw/3>
- Listed in the **Best Computer Science Scientists database maintained by Research.com**, a leading academic platform for researchers, with **World Ranking: 1650 and National Ranking (India): 8**.
- **Visiting Faculty at the Old Dominion University (ODU), Suffolk, VA 23435, USA, with the Virginia Modeling, Analysis, and Simulation Center (VMASC) [Duration: 1 May 2022 - 30 June 2022]**.
- **More detailed information at:**
<https://sites.google.com/view/iitkgpakdas/>

- **Sajal K. Das**, IEEE Fellow, Professor and Daniel St. Clair Endowed Chair, Department of Computer Science, Missouri University of Science and Technology, Rolla, MO 65409, USA
- **Mauro Conti**, IEEE Fellow, Head of SPRITZ Security and Privacy Research Group, Director of UniPD node of CINI Cybersecurity National Lab, EU Marie Curie Fellow Alumni, CEO and co-funder of CHISITO, and Co-funder of DYALOGHI, University of Padua, Italy
- **Willy Susilo**, IEEE Fellow, ARC Future Fellow, Co-Director, Centre for Computer and Information Security Research, University of Wollongong, AUSTRALIA
- **Sherali Zeadally**, Fellow of the British Computer Society and the Institution of Engineering Technology, Stevenage, U.K., University of Kentucky, Lexington, KY 405 06 USA
- **Kim-Kwang Raymond Choo**, Fellow, Australian Computer Society, Department of Information Systems and Cyber Security, The University of Texas at San Antonio, San Antonio, TX 78249 USA
- **Xinyi Huang**, Fujian Provincial Key Laboratory of Network Security and Cryptology, Fujian Normal University, Fuzhou, Fujian, China
- **Alexey Vinel**, Halmstad University, Halmstad, Sweden
- **Muhammad Khurram Khan**, FIET (UK), FBCS (UK), Center of Excellence in Information Assurance, King Saud University, Riyadh, Saudi Arabia

- **Athanasios V. Vasilakos**, Lulea University of Technology, Sweden
- **Minho Jo**, Department of Computer and Information Science, Korea University, Seoul, South Korea
- **Laurence T. Yang**, St. Francis Xavier University, Canada
- **Joel J. P. C. Rodrigues**, IEEE Fellow, National Institute of Telecommunications - Inatel, Brazil
- **Debiao He**, School of Cyber Science and Engineering, Wuhan University, Wuhan 430 072, China
- **Jong-Hyouk Lee**, Sangmyung University, Republic of Korea
- **Kee-Young Yoo**, Kyungpook National University, Daegu, Korea
- **Qi Jiang**, Xidian University, China
- **Sachin Shetty**, Old Dominion University, USA
- **Xiong Li**, Hunan University of Science and Technology, China
- **Mamoun Alazab**, Charles Darwin University, Australia
- **Mohammad S. Obaidat**, IEEE Fellow, University of Sharjah
- **YoungHo Park**, School of Electronics Engineering, Kyungpook National University, South Korea
- **Mohsen Guizani**, IEEE Fellow, Mohamed Bin Zayed University of Artificial Intelligence (MBZUAI)

● Part 1: Basics of Cryptography

- ▶ Cryptographic goals and objectives
- ▶ Types of attacks, passive and active attacks
- ▶ Introduction to Number Theory
- ▶ Complexity Theoretic Connections
- ▶ Overview of symmetric and public key cryptography
- ▶ Digital Signatures

● Part 2: Basics of System Security

- ▶ Intruders: Intruders, Intrusion detection, Intrusion prevention.
- ▶ Software Vulnerabilities: Phishing, Buffer overflow (BOF), Heap overflow, Format string attacks, Cross-site scripting (XSS), SQL Injection.

● Part 3: Basics of Network Security

- ▶ Overview of encrypting communication channels
- ▶ Overview of various security protocols at OSI layers
- ▶ **Introduction to IoT security:** IoT architecture, various IoT applications, security requirements, security attacks, threat model for the IoT ecosystem, taxonomy of security protocols
- ▶ **Introduction to Blockchain technology:** Various applications of blockchain of Things (BCoT), centralized versus decentralized models, types of blockchain, brief overview of various consensus algorithms, block formation and addition in a blockchain
- ▶ **AI/ML Security**

- William Stallings, “Cryptography and Network Security: Principles and Practices,” Pearson Education, 6th Edition, 2014.
- Bernard Menezes, “Network Security and Cryptography,” Cengage Learning, 2010.
- Behrouz A. Forouzan, “Cryptography and Network Security,” Special Indian Edition, 2010.

Grading Method:: Relative

- Quiz: 30
- End Sem Exam: 50
- Assignments: 20

Thank You!!!