About this course

Cryptography provides the underlying security methods for the web and many other computer applications. This course covers the design usage of cryptographic protocols for online and offline computing applications. Assuring the quality, validity and privacy of information is one of the key applications of Cryptography. Applications of cryptography ranges from signatures and certificates to trustless multiparty computations.

Specific topics covered include:
- Large numbers, random numbers, hash functions and number theory
- Encryption methods and common ciphers
- Password storage and password cracking
- Authentication, key exchange and man in the middle (MITM) attacks
- Secure messaging, Kerberos and Secure Sockets Layer (SSL) or Transport Level Security (TLS)
- RSA and why it works
- Advanced cryptographic protocols
- Anonymity, money and secure election algorithms

Required prior knowledge and skills

- Algorithms
- Data Structures
- Computer Organization
- Operating Systems
- Programming using C or C++ using Linux (Python or Java is useful)

Learning Outcomes

Learners completing this course will be able to:
- Differentiate the major algorithmic techniques used in cryptography
- Explain the concept and correctness of cryptographic protocols
- Perform identification of vulnerabilities in systems
- Explain the algorithms used for constructing cryptographic computations
- Perform steps needed for encryption, authentication, integrity, certification and data privacy
- Explain complex protocols that involve many steps and computing agents who do not trust each other

Estimated Workload/Time Commitment Per Week

15 - 20 hours per week

Technology Requirements

Hardware - Standard with major OS
Software and Other (programs, platforms, services, etc.) - Virtual Machine running 32 bit Linux
Dr. Partha Dasgupta
Dr. Partha Dasgupta is an Associate Professor in the School of Computing, Informatics, and Decision Systems Engineering at Arizona State University (ASU). His core areas of expertise are in Computer Security, Cryptography and Operating Systems. His current research focus is the use of cryptography and secure software systems to provide security and dependability of consumer computing. He has significant prior research results and publications in construction of distributed operating systems, high performance systems and secure computing infrastructures. In addition to ASU, Dr. Dasgupta has held faculty positions at Georgia Tech and New York University.