CSE 4137: Cryptography and Security

Course Teacher: Mosarrat Jahan, Associate Professor, Department of Computer Science and Engineering, University of Dhaka.

With the explosive growth of the internet, the advent of various computing paradigms, availability of cost-effective computing devices and pervasive usages of resource-constrained IoT devices, user data nowadays are handled in many innovative ways. Although these facilities provide the ease of data usages to the users, the mechanism of handling data is not very clear to the users, and often proper security measures are missing leading to the growing number incidents of data breaches. This signifies the need to increase the awareness of the need to protect data from unwanted disclosure, to assure the authenticity of data, and to protect systems from various types of network-based attacks. Cryptographic tools are fundamental building blocks to protect data from unauthorized usage. Although initially developed for protecting sensitive information from enemies in the battlefield, the cryptographic tools have become matured over time and used as necessary security protocols in many applications such as user authentication, access control, crypto currency, block chains, etc.

Course Objectives:

This course introduces the concepts of various security issues and existing preventative measures and basic cryptographic protocols to the beginners. In particular, the objectives are

1. To understand basics of Cryptography and Information Security.
2. To learn how to maintain the Confidentiality, Authenticity, Integrity and Availability of data.
3. To gain knowledge of existing internet security protocols.
4. To understand the operating system and application level security concepts.
5. To learn about various legal and ethical issues of computer security.

Course Outcomes:

After successful completion of the course, the learners will be

1. Aware of various security threats to data and can protect them.
2. Ready to gain advanced knowledge on different topics covered in this course leading to research in the emerging areas of cryptography and network security.
3. Implement various networking protocols and will be able to apply them to solve existing open research problems.

4. Ready for the industry oriented development by gaining thorough knowledge especially on the operating system, application level, database level security and cryptography.
5. Ready for more advanced courses in security track.

Some Application Area:

1. With the advent of many exciting applications of low-powered devices such as smart phones, tablets, sensors and various IoT devices, it becomes essential to integrate these devices in the computing environment. Currently, an active area of research is to devise light-weight cryptographic schemes to ensure data security for these devices that can match up their limited capacity of processing power, storage space and battery power. Many security problems are still not explored in mobile cloud computing, fog computing, wireless body area networking, Internet of Things, smart cities, etc. that need the application of suitable light-weight cryptographic schemes.

2. Cryptography also plays a vital role in the industry-oriented development of applications to ensure information security. Few examples include the development of secure email system, safe payment system, secure database management tool, secure logging system, secure e-health system, etc.