# COT 4930 Applied Cryptography

**Credits:** 3 credits

**Textbook, Title, Author and Year:** Introduction to Modern Cryptography (2nd edition), Katz and Lindell, Chapman & Hall/CRC.

**Reference Materials:** Cryptography Theory and Practice (3$^{rd}$ edition), Stinson, Chapman & Hall/CRC. Handbook of Applied Cryptography, Menezes, Oorschot, Vanstone, Chapman & Hall/CRC.

**Specific Course Information**

a. **Catalog Description:** This is a course on applied cryptography. The following components are covered in the course: (a) Mathematical background, (b) Basic algorithmic number theory, (c) Introduction and classical cryptography, (d) Private-key (symmetric) cryptography, (e) Public-key (asymmetric) cryptography, and (f) Advanced topics on applied cryptography.

b. **Prerequisites:** MAD2104 and COP3014. Knowledge of linear algebra, number theory and computer programming would be of great help. The instructor also reviews some of the necessary background materials.

**c.** **Specific Goals for the Course:** This course enables the students to learn the mathematical aspects of applied cryptography and the fundamental concepts of cryptographic algorithms. Furthermore, it enables the students to utilize these techniques in computing systems.

**Brief List of Topics to be Covered**

In the first part of the course, the following concepts and topics will be covered with different levels of emphasis. Some topics will be covered in-depth and some other topics will be reviewed briefly.

1. Mathematical Background
2. Basic Algorithmic Number Theory
3. Introduction and Classical Cryptography
4. Private-Key (Symmetric) Cryptography
5. Public-Key (Asymmetric) Cryptography

In the second part of the course, the instructor and students will discuss advanced topics on applied cryptography. Topics of interest include (but are not limited to):

6. Cryptographic Primitives
7. Secure Multiparty Computation
8. Privacy-Preserving Protocols
9. Homomorphic Encryption
10. Rational Cryptography