SM-3401 Cryptography

Module Code :	SM-3401		
Module Title :	Cryptography		
Type of Module :	Breadth		
Modular Credits :	2	**Student Workload:** **Contact hours for timetabling :**	4-5 hours/week 2 hours / week
Prerequisite :	None		
Anti-requisite :	SM-4326		

Aims:

Cryptography is the study and practice of hiding information. Modern cryptography intersects the discipline of Mathematics, Computer Science and Engineering. This course lays down the mathematical foundation of cryptography and coding theory and offers many practical examples.

Upon completion of this course, students should be able to describe ancient and modern encryption methods, encode and decode information using simple monoalphabetic substitution ciphers, polyalphabetic substitution codes such as Vigenere code and the RSA code. They should also be able to write computer programs for encrypting and decrypting information using different cryptosystems.

Module Content:

- History of cryptography: Encryption and decryption of cipher systems; Different cryptosystems including mono alphabetic and polyalphabetic substitution ciphers, the Vigenere code; use of cryptography during the world wars including the Enigma code; DES code.
- Public Key Cryptography: The key exchange problem; Diffe-Hellman-Merkele key exchange system; the RSA code and the mathematics behind it; digital signatures and Internet security.

Assessment:	Examination: 60%	Course Work: 40% (Two class tests, 15% each, 1 assignment 10%.)