MAT 661 – Coding Theory & Cryptography

Course Code & Number	Course Name	Credit Hours	Lec.	Lab.	Tut.	Prerequisites
MAT 661	Coding Theory & Cryptography	4	3	0	1	MAT 623

Syllabus:

Basics and Linear Codes: Error detection, correction and decoding, Hamming distance and Distance of a code, MLD reliability, Linear Codes and their Basis, Generator matrix and parity-check matrix, Equivalence of linear codes, Encoding with a linear codes, Cosets of Linear Codes and the coset leader, Nearest neighbor decoding.

Bounds and Constructions of linear Codes: Optimal codes, extended codes and parity-check matrices, Bounds for codes and their types, Perfect Codes, Hamming Codes and their use, Golay Codes, Reed-Muller Codes and their use.

Cyclic Codes and Other Codes: Cuclic hamming codes, BCH Codes and their use, Codes over GF(2^n), Reed-Solomon Codes, Quadratic-residue Codes, Hadamard matrix codes, Nordstrom, Robinson code, Preparata codes and Kerdock codes, Propagation rules of constructing Linear Codes, First order and higher Reed-Muller codes, Subfield Codes.

Classic Cryptography: Encryption Schemes, Symmetric key encryption, Fiestel Cipher and DES.

Public-Key Cryptography: (PKC): Algorithm and Complexity, Quadratic residues and quadratic reciprocity, Partiality testing, Discrete algorithm, Hash functions, RSA, Provable security and EL-Gamal, Cryptography Protocols (Diffe Hellman, Zero Knowledge and coin-tossing).

References:

1. D. Hankerson and others; ***Coding Theory and Cryptography*: *The Essentials***; 2nd Edition, Marcel Dekker, 2000. **(Main Reference)**
2. S. Ling and C. Xing; ***Coding Theory: A First Course***; 1st Edition, Cambridge University Press, 2004.
3. J. van Lint; ***Introduction to Coding Theory***; 3rd Edition, Springer, 1998.
4. Shu Lin and D. Castello; ***Error Correcting Codes***; 2nd Edition, Prentice Hal, 2004.