KINGDOM OF SAUDI ARABIA
AL-IMAM MOHAMMAD BIN SAUD
ISLAMIC UNIVERSITY
FACULTY OF SCIENCES
DEPARTMENT OF MATHEMATICS

المملكة العربية السعودية
جامعة الإمام محمد بن سعود الإسلامية
كلية العلوم
قسم الرياضيات والإحصاء

Introd. to Cryptography and Coding

Course Code	Course Num.	Course Name	Credit Hours	Lec	Lab	Tut	Prerequisites
MAT	461	Introd. to Cryptography and Coding	4	3	0	2	MAT 321

Objectives :

This course is divided in two parts: Cryptography and Coding Theory.
The objective of the first part is to learn students basics of Cryptography through classical ciphers, cryptanalysis and some applications.
The objective of the second part is to introduce students to elementary coding theory.

Syllabus:

Cryptography:

- **Classical Ciphers**: Shift ciphers ،affine ciphers and substitution ciphers. Introduction to stream ciphers ،including linear recursive ciphers.
- **Introduction to cryptanalysis:** the four levels of attack: known ciphertext, known plaintext, chosen plaintext and chosen ciphertext. Exponential ciphers and key distribution. Public-key cryptosystems: RSA, ElGamal and Massey-Omura. Signature schemes with applications.

Coding Theory:

- **Introduction to codes:** Error-detection ،error correction and information rate. Linear codes, Perfect codes. Cyclic codes.

References:

- **Introduction to Modern Cryptography** byJ. Katz and Y. Lindell, Chapman and Hall/CRC, 1st Edition(2007)
- **Elementary Number Theory** by K. Rosen ،Addison Wesley; 5th Edition (2004).
- **A First Course in Coding Theory**، by R. Hill, OxfordUniversity Press (1997).
- **Coding Theory: A First Course** by San Ling and Chaoping Xing, CambridgeUniversity Press (2004).