

Topics covered in MATH3302

Cryptography

1. Introduction to Cryptography

Covers basic concepts, history, different types of cryptosystems.

2. Classical Cryptography

Covers classical ciphers: Mixed alphabet, Vigenere, Playfair, Hill, Permutation ciphers, AD-FGVX, Stream cipher.

3. Shannon's Theory

Covers measures of security, probability, perfect secrecy, one-time pads and random number generation.

4. Substitution-Permutation Ciphers

Covers substitution-permutation ciphers (product ciphers), feistel ciphers.

5. The Data Encryption Standard (DES)

Covers the encryption and decryption processes for DES, applications of DES, variants and weaknesses.

6. IDEA

Covers the encryption and decryption processes for IDEA, cryptanalysis of IDEA.

7. AES: Rijndael

Covers the background of the development of the Advanced Encryption Standard, the mathematics behind AES, and its use.

8. Public Key Cryptography

Covers some number theory, the encryption and decryption processes for RSA, cryptanalysis of RSA, and its use.

Coding Theory

1. Background for coding theory

Covers linear algebra background (independent study, not covered in class).

2. Introduction to coding theory

Covers basic concepts, error detection and correction, maximum likelihood decoding.

3. Linear codes I

Covers general linear codes, generating matrices, parity check matrices, and maximum likelihood decoding for linear codes.

4. Linear codes II

Covers bounds for codes, extended code construction, Hamming codes, Reed-Muller codes, (extended) Golay code.

5. Cyclic Codes

Covers burst errors, generating polynomials for cyclic codes, error detection and correction for cyclic codes, interleaving (compact discs).