

## Review Questions for Midterm Exam CSE 40622/60622 Fall 2009

1. Encryption: the objective, types of encryption algorithms, adversarial models.
2. Historical ciphers: shift and substitution ciphers, monoalphabetic and polyalphabetic ciphers, cryptanalytic techniques against such ciphers.
3. Perfect secrecy: definitions, interpretation, one-time pad; the notion of entropy, rate of a natural language.
4. Symmetric key encryption in the presence of eavesdropping adversaries: security definitions and techniques, pseudorandom generators.
5. Security against chosen plaintext attacks for symmetric key encryption: definitions, constructions, pseudorandom functions.
6. Symmetric key block ciphers: confusion-diffusion paradigm and substitution-permutation networks, Feistel structure, DES and AES (security, performance).
7. Encryption modes for long messages, their properties.
8. Data integrity or data origin authentication: the objective, message authentication codes for fixed-length and variable-length messages, theoretical and practical constructions.
9. Hash functions: security properties, Merkle-Damgard construction, practical algorithms and standards.