**Introduction to Cryptography with Coding Theory**

Chapter 1: Overview of Cryptography and Its Applications

* **Cryptology**: study of communication over nonsecure channels.
* **Cryptography**: process of designing cryptologic systems.
* **Cryptanalysis**: breaking cryptographic systems.
* **Coding theory**
* Representing input information symbols by output symbols called code symbols
* Covers compression, secrecy, error correction
* Possible attacks
* Cyphertext only
* Known plaintext (cribs)
* Chosen plaintext: temporary access to encryption machine to deduce key. Eve can put plaintext into system and get ciphertext (can encrypt)
* Chosen cyphertext: access to decryption machine to deduce key. Eve can derive plaintext from ciphertext (can decrypt)
* **Kerckhoff's principle:** one should always assume the enemy knows the encryption method being used when assessing the security of a cryptosystem.
* Symmetric and Public Key algorithms
* **Symmetric Key**. Encryption and decryption keys both known to both parties.
* **Steam ciphers.** Data fed into algorithm in small pieces (bits, chars) and output is returned in small pieces.
* **Block ciphers.** Block of input bits collected and all at once and output as block.
* **Public Key.** Encryption key is public, but decryption key infeasible to find without information known only to receiving party. RSA is the most popular implementation of this.
* Public key encryption more computationally expensive, and generally not used to encrypt large quantities of data.
* **Codes:** words and letter combinations are replaced by code words.
* **Cipher:** encrypts every string of characters via algorithm.
* Factorization takes significantly longer than multiplication.

Chapter 2: Classical Cryptosystems.

* **Shift cipher (Caesar cipher).** x --> x + k, where k = the key.
* **Affine cipher.** Shift cipher variation. x --> ax + b, where gcd(a, 26) = 1.
* **Vigenère cipher.** Shift cipher variation. Key is a vector representative of a word of length n. For instance, the key k = vector = (21,4,2,). Encrypt by shifting first letter of plaintext by k[0], second letter by k[1], etc. After k[n-1] go back to k[0].

Lectures

* If a + b = 0 (mod 26), then we say that b is a's additive inverse

e.g. the additive inverse of 5 is 21 (mod 26)

* Multiplicative inverse of a is the value b such that a \* b = 1 mod 26