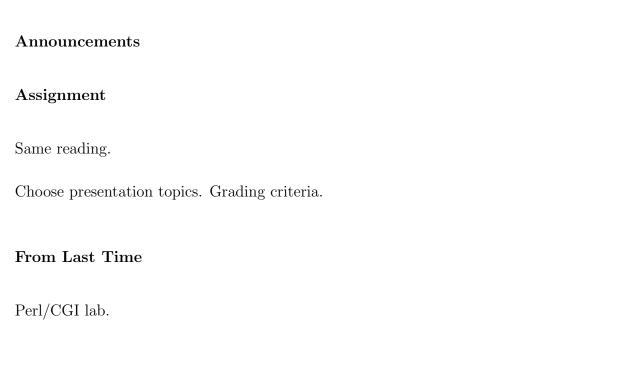
# Introduction to Cryptography

Tom Kelliher, CS 325 Feb. 8, 2010

### 1 Administrivia



#### Outline

- 1. Basic terminology.
- 2. Substitution.
- 3. Transposition.
- 4. What makes a good cipher?

### Coming Up

More Cryptography.

## 2 Basic Terminology

- 1. Plain text, cipher text.
- 2. Key.
- 3. Interceptor aims: block, intercept, modify, fabricate.
- 4. Symmetric cipher: P = D(K, E(K, P)).

One key. Key distribution and management issues. Private key cryptography.

5. Asymmetric cipher:  $P = D(K_d, E(K_e, P))$ .

Two keys: private and public. Public key cryptography.

6. Product Ciphers — application of two or more ciphers:  $C = E_2(K_2, E_1(K_1, P))$ .

The result is not necessarily "better."

7. Diffusion: A plain text character has a functional impact on multiple cipher text characters.

This forces the cryptanalyst to have access to large amounts of cipher text.

8. Confusion: A cryptanalyst should not be able to predict the changes that occur when one character of the plain text is changed. (Consider a Caesar cipher.)

This property makes it harder to understand the relationship between the plain text and the cipher text.

9. Stream cipher: One plain text character is used to produce one cipher text character.

Fast; no latency.

Poor diffusion; possibly little confusion.

10. Block cipher: A block of plain text is used to produce a block of cipher text.

Slower; latency.

Excellent diffusion and confusion.

### 3 Substitution

- 1. Exchange one character for another, using a table. Many variations.
- 2. Simple examples: Caesar rotation, ROT13.
- 3. Permutation and keys. 26! possible permutations.

Simple permutation scheme using "tolerant" as key: toleranbcdfgh... (Use key and follow up with remaining letters.)

- 4. One time pad. Components:
  - (a) A set of n permutations.
  - (b) An infinite string of random numbers, modulo n.

For each plaintext character, use the next random number to select the permutation to apply.

Keeping the pads in synch.

5. Other methods: Vernam cipher, book cipher.

# 4 Transposition

- 1. Columnar technique.
- 2. Re-arrange the plaintext characters.
- 3. Primitive example: Pig Latin.

4.	General	idea:

- (a) Construct a matrix with n columns.
- (b) Length of plain text should be cn. If not, pad out.
- (c) Write plain text across rows of matrix.
- (d) Read cipher text across columns of matrix.

# 5 What Makes a Good Cipher?

#### 1. According to Shannon:

- (a) Amount of secrecy should be proportional to amount of labor.
- (b) Keys, algorithms should be free from complexity.
- (c) Implementation process should be KISS.
- (d) Error in encrypting should not propagate.
- (e) Length of cipher text should match length of plain text.

### $2. \ \ \hbox{``Trustworthy'' encryption:}$

- (a) Based on sound mathematics.
- (b) Analyzed by experts and found to be sound.
- (c) Has withstood the "test of time."