Classical Encryption Techniques

Raj Jain
Washington University in Saint Louis
Saint Louis, MO 63130
Jain@cse.wustl.edu

Audio/Video recordings of this lecture are available at:
http://www.cse.wustl.edu/~jain/cse571-11/
Overview

1. Symmetric Cipher Model
2. Substitution Techniques
3. Transposition Techniques
4. Product Ciphers
5. Steganography

Symmetric Cipher Model

\[ Y = E(K, X) \]
\[ X = D(K, Y) \]

K = Secret Key
Same key is used for encryption and decryption.
⇒ Single-key or private key encryption.
Some Basic Terminology

- **Plaintext** - original message
- **Ciphertext** - coded message
- **Cipher** - algorithm for transforming plaintext to ciphertext
- **Key** - info used in cipher known only to sender/receiver
- **Encipher (encrypt)** - converting plaintext to ciphertext
- **Decipher (decrypt)** - recovering ciphertext from plaintext
- **Cryptography** - study of encryption principles/methods
- **Cryptanalysis (code breaking)** - study of principles/methods of deciphering ciphertext *without* knowing key
- **Cryptology** - field of both cryptography and cryptanalysis
Cryptography Classification

- **By type of encryption operations used**
  - Substitution
  - Transposition
  - Product

- **By number of keys used**
  - Single-key or private
  - Two-key or public

- **By the way in which plaintext is processed**
  - Block
  - Stream
Cryptanalysis

- **Objective:** To recover key not just message
- **Approaches:**
  - Cryptanalytic attack
  - Brute-force attack
- If either succeed all key use is compromised
- **Brute-force attack:**

<table>
<thead>
<tr>
<th>Key Size (bits)</th>
<th>Number of Alternative Keys</th>
<th>Time required at 1 decryption/µs</th>
<th>Time required at $10^6$ decryptions/µs</th>
</tr>
</thead>
<tbody>
<tr>
<td>32</td>
<td>$2^{32} = 4.3 \times 10^9$</td>
<td>$2^{31}$ µs</td>
<td>= 35.8 minutes</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2.15 milliseconds</td>
</tr>
<tr>
<td>56</td>
<td>$2^{56} = 7.2 \times 10^{16}$</td>
<td>$2^{55}$ µs</td>
<td>= 1142 years</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>10.01 hours</td>
</tr>
<tr>
<td>128</td>
<td>$2^{128} = 3.4 \times 10^{38}$</td>
<td>$2^{127}$ µs</td>
<td>= $5.4 \times 10^{24}$ years</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>5.4 $\times 10^{18}$ years</td>
</tr>
<tr>
<td>168</td>
<td>$2^{168} = 3.7 \times 10^{50}$</td>
<td>$2^{167}$ µs</td>
<td>= $5.9 \times 10^{36}$ years</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>5.9 $\times 10^{30}$ years</td>
</tr>
<tr>
<td>26 characters (permutation)</td>
<td>$26! = 4 \times 10^{26}$</td>
<td>$2 \times 10^{26}$ µs</td>
<td>= $6.4 \times 10^{12}$ years</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>6.4 $\times 10^6$ years</td>
</tr>
</tbody>
</table>
Substitution

- Caesar Cipher: Replaces each letter by 3rd letter on
  
  Example:
  
  meet me after the toga party
  PHHW PH DIWHU WKH WRJD SDUWB

- Can define transformation as:
  
  a b c d e f g h i j k l m n o p q r s t u v w x y z
  D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

- Mathematically give each letter a number
  
  a b c d e f g h i j k l m n o p q r s t u v w x y z
  0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

- Then have Caesar cipher as:
  
  \[ c = E(k, p) = (p + k) \mod (26) \]
  \[ p = D(k, c) = (c - k) \mod (26) \]

- Weakness: Total 26 keys
Substitution: Other forms

- Random substitution:
  Plain:  abcdefghijklmnopqrstuvwxyz
  Cipher: DKVQFIBJWPESCMXHTMYAULRGZN
  The key is 26 character long
  => 26! (= 4 \times 10^{26}) Keys in place of 26 keys

- Letter frequencies to find common letters: E,T,R,N,I,O,A,S
Substitution: Other forms (Cont)

- Use two-letter combinations: Playfair Cipher
- Use multiple letter combinations: Hill Cipher
Poly-alphabetic Substitution Ciphers

- Use multiple ciphers. Use a key to select which alphabet (code) is used for each letter of the message.
- Vigenère Cipher: Example using keyword *deceptive*
  
  key: deceptionedeciphertext: ZICVTWQNGRZGVTWAVZHCQYGLMGJ
One-Time Pad

- If a truly random key as long as the message is used, the cipher will be secure
- Called a One-Time pad
- Is unbreakable since ciphertext bears no statistical relationship to the plaintext
- Since for any plaintext & any ciphertext there exists a key mapping one to other
- Can only use the key once though
- Problems in generation & safe distribution of key
Transposition (Permutation) Ciphers

- Rearrange the letter order without altering the actual letters
- **Rail Fence Cipher**: Write message out diagonally as:
  - `mematrhgpry`  
  - `etefetecaat`
- Giving ciphertext: `MEMATRHTGPRYETEFETEOAAT`
- **Row Transposition Ciphers**: Write letters in rows, reorder the columns according to the key before reading off.
  - **Key**: 4312567
  - Column Out: 4 3 1 2 5 6 7
  - Plaintext: `attackpoint`
  - Ciphertext: `TTNAAPTMTSUOAODWCOIXKNLYPETZ`
Product Ciphers

- Use several ciphers in succession to make harder, but:
  - Two substitutions make a more complex substitution
  - Two transpositions make more complex transposition
  - But a substitution followed by a transposition makes a new much harder cipher

- This is a bridge from classical to modern ciphers
Rotor Machines

- Before modern ciphers, rotor machines were most common complex ciphers in use
- Widely used in WW2
  - German Enigma, Allied Hagelin, Japanese Purple
- Implemented a very complex, varying substitution cipher
- Used a series of cylinders, each giving one substitution, which rotated and changed after each letter was encrypted

Hagelin Rotor Machine
A becomes Y (First rotor). Y becomes R (2nd rotor). R becomes B (3rd rotor).

After each letter, first rotor moves 1 position. After each full rotation of 1st rotor, 2nd rotor moves by 1 position.

Cycle length = $26^3$
Steganography

- Hide characters in a text, hide bits in a photograph
- Least significant bit (lsb) of a digital photograph may be a message.
- Drawback: high overhead to hide relatively few info bits
- Advantage: Can obscure encryption use

Ref: http://www.cse.wustl.edu/~jain/cse571-09/ftp/stegano/index.html
Summary

1. The key methods for cryptography are: Substitution and transposition
2. Letter frequency can be used to break substitution
3. Substitution can be extended to multiple letters and multiple ciphers. Mono-alphabetic=1 cipher, Poly-alphabetic=multiple ciphers
4. Examples: Caesar cipher (1 letter substitution), Playfair (2-letter), Hill (multiple letters), Vigenere (poly-alphabetic).
5. Multiple stages of substitution and transposition can be used to form strong ciphers.
Submit solution to problem 2.18

This problem explores the use of a one-time pad version of the Vigenere cipher. In this scheme, the key is a stream of random numbers between 0 and 26. For example, if the key is 3 19 5…, then the first letter of the plaintext is encrypted with a shift of 3 letters, the second with a shift of 19 letters, the third with a shift of 5 letters, and so on.

A. Encrypt the plain text sendmoremoney with the key stream 9 0 1 7 23 15 21 14 11 11 2 8 9

B. Using the ciphertext produced in part (a), find a key so that the cipher text decrypts to the plain text cashnotneeded.