Basic Cryptography

Week 3, Tuesday

What’s Cryptography

• A deep mathematical subject
• Viewed as a supporting tool in the eyes of computer security scientist
• A cornerstone for secure communication

Definitions

• **Cryptography**: the art and science of concealing information
• **Cryptoanalysis**: code breaking
• **Cryptosystem**: basic component of cryptography
  - \( \{ \mathbf{E}, \mathbf{D}, \mathbf{M}, \mathbf{K}, \mathbf{C} \} \)
  - \( \mathbf{M} \): plaintexts
  - \( \mathbf{K} \): keys
  - \( \mathbf{C} \): ciphertexts
  - \( \mathbf{E} \): enciphering functions \( \mathbf{M} \times \mathbf{K} \rightarrow \mathbf{C} \)
  - \( \mathbf{D} \): deciphering functions \( \mathbf{C} \times \mathbf{K} \rightarrow \mathbf{M} \)

Caesar Cipher

• Letters are shifted
  - If key is 3, then A becomes D, B becomes E, Z becomes C
  - If key is 0, “Caesar” become “Fdhvdu”

  Here,
  - \( \mathbf{M} = \{ \text{all sequence of Roman letters} \} \)
  - \( \mathbf{K} = \{ \text{an integer such that } 0 \leq I \leq 25 \} \)
  - \( \mathbf{E} = \{ \mathbf{E}(i, k) \text{ and for all } m \in \mathbf{M}, \mathbf{E}(m) = (m+k) \text{ mod } 26 \} \)
  - \( \mathbf{D} = \{ \mathbf{D}(c, k) \text{ and for all } c \in \mathbf{C}, \mathbf{D}(c) = (26+c-k) \text{ mod } 26 \} \)
  - \( \mathbf{C} = \mathbf{M} \)

Goal of Cryptography

• Keep enciphered info secret

• Standard assumptions of attackers:
  - Knows the algorithm
  - Does NOT know the key

Encryption Attack Types

• **Ciphertext only attack**
  - Know: ciphertext
  - Goal: what’s the plaintext?

• **Known plaintext attack**
  - Know: (all the) ciphertext and plaintext
  - Goal: what’s the key?

• **Chosen plaintext attack**
  - Know: chosen plaintext and its ciphertext
  - Goal: What’s the key?
What Does an Attacker Know

- Well, mathematics and statistics
  - 1-gram model of English text, or 2-gram, Markov model, word model, etc.
- Learn the statistics of plaintext
- Examine the ciphertext
- Correlate the statistical info of ciphertext and plaintext

Classical Cryptosystems

- Same key for encryption and decryption
  - Also called single-key cryptosystem
  - Or symmetric cryptosystem
- For all $E_k \in E$ there is $D_k \in D$ such that
  $$D_k = E_k^{-1}$$
- Two basic classical ciphers
  - Transposition
  - Substitution

Transposition Cipher

- Characters in plaintext are rearranged
  - Letters unchanged
- Rail fence cipher, as an example
  - "UNIV OF OREGON" becomes
  ```
  UI O OEO UVFRO
  NV F RGN N EN
  IOOG
  ```

Cryptoanalysis of Transposition

- 1-gram frequencies match plain English, but 2-gram does not
  - Probably a transposition cipher
- Anagramming
  - In above example, who has the highest probability to follow letter "U"?
  - Konheim’s diagram table says “N”
  - So what?

Substitution Cipher

- Characters are changed
  - Caesar cipher for example
- Cryptoanalysis
  - Calculate the correlation function between the frequency of each letter in ciphertext and that in English

Vigenere Cipher

- Use a longer key to obscure the statistics
- The length of a key is called the period of the cipher
- A tableau is used to implement cipher
  - Table lookup for encryption
(cont’d)

Key B ENCHBENC HBENCH
Plaintext A LIMERICK PACKS LAUGHS
Ciphertext B PVOLSMFM WBGXU SBYTJZ

Cryptoanalysis of Vigenere Cipher

• Considered unbreakable for many years, until...
• Look at an example below
  Key VIGVIGVIGVIG
  Plaintext THEBOYHASTHEBAG
  Ciphertext OPKWWECIYOPKNIM
• Repitions when key letters appear over the same letters in the plaintext
  – Attackers can look for multiple repetitions
  – Then the attacker can guess the period
• For example, repetitions after 6 letters and 9 letters, then period=3.

(continued)

Key VIGVIGVIGVIGVIG
Plaintext THEBOYHASTHEBAG
Ciphertext OPKWWECIYOPKNIM

Knowing the period, we now can look at each key letter separately
And solve it as a Caesar cipher.

One-Time Pad

• A variant of the Vigenere cipher
• Same technique
• Key string is randomly chosen and at least as long the message!
  – No repetition
• Impossible to break! Perfect secrecy :)
  – Impossible to deploy either. :(  [Page 228-230] Figure 9-5.6.7

DES: Data Encryption Standard

• A classical cryptosystem
• Bit-level
• Uses both transposition and substitution
  – Also referred as product cipher
• Encipherment unit: 64-bit blocks
  – Input, output and keys are all in 64b blocks

How Does DES Work

• You don’t have to remember those details
  – You will forget anyway
  – You cannot remember it either probably
• Let’s just go through it for fun
  – [Page 228-230] Figure 9-5.6.7
Three Common Modes of DES

- CBC: Cipher Block Chaining
- EDE: Encrypt-Decrypt-Encrypt
- Triple DES: DES-DES-DES

EDE

- Two 64-bit keys: $k$ and $k'$

$$c = DES_k(DES_{k'}^{-1}(DES_k(m)))$$

Triple DES

- Three 64-bit keys: $k$, $k'$, and $k''$

$$c = DES_k(DES_{k'}(DES_{k''}(m)))$$

Breaking DES

- 1977. Diffie and Hellman: designed a $20M$ machine to break it in a matter of days
- 1990. Biham and Shamir applied differential cryptanalysis
- 1998. Computers distributed throughout the Internet

AES: Advanced Encryption Standard

- DES is no longer as secure as designed in its early days
- 2001. NIST selects Rijndael as AES.