Cryptography: Terminology & Classic Ciphers
Announcements

- Join class mailing list: CS426_Fall2010@cs.purdue.edu
Security Goals

• Confidentiality (secrecy, privacy)
  – only those who are authorized to know can know

• Integrity
  – only modified by authorized parties and in authorized ways

• Availability
  – those authorized to access can get access
Tools for Information Security

- Cryptography
- Access control
- Hardware/software architecture for separation
- Processes and tools for developing more secure software
- Monitoring and analysis
- Recovery and response
Goals of Cryptography

- The most fundamental problem cryptography addresses: ensure security of communication over insecure medium
- What does secure communication mean?
  - confidentiality (privacy, secrecy)
    - only the intended recipient can see the communication
  - integrity (authenticity)
    - the communication is generated by the alleged sender
- What does insecure medium mean?
  - the adversary can eavesdrop
  - the adversary has full control over the communications
Approaches to Secure Communication

- Steganography
  - “covered writing”
  - hides the existence of a message
  - depends on secrecy of method

- Cryptography
  - “hidden writing”
  - hide the meaning of a message
  - depends on secrecy of a short key, not method
Cryptography, cryptanalysis, and cryptology

- **Cryptography**,
  - Traditionally, designing algorithms/protocols
  - Nowadays, often synonym with cryptology

- **Cryptanalysis**
  - Breaking cryptography

- **Cryptology: both cryptography & cryptanalysis**
  - Becoming less common,
History of Cryptography

- 2500+ years
- An ongoing battle between codemakers and codebreakers
- Driven by communication & computation technology
  - paper and ink
  - cryptographic engine & telegram, radio
  - modern cryptography: computers & digital communication
Basic Terminology

- Plaintext: original message
- Ciphertext: transformed message
- Key: secret used in transformation
- Encryption
- Decryption
- Cipher: algorithm for encryption/decryption
Shift Cipher

- The Key Space:
  - [1 .. 25]
- Encryption given a key $K$:
  - each letter in the plaintext $P$ is replaced with the $K$’th letter following corresponding number (shift right)
- Decryption given $K$:
  - shift left

History: $K = 3$, Caesar’s cipher
Shift Cipher: Cryptanalysis

• Can an attacker find $K$?
  – YES: by a brute force attack through exhaustive key search,
  – key space is small (<= 26 possible keys).

• Once $K$ is found, very easy to decrypt
General Mono-alphabetic Substitution Cipher

• The key space: all permutations of $\Sigma = \{A, B, C, \ldots, Z\}$

• Encryption given a key $\pi$:
  – each letter $X$ in the plaintext $P$ is replaced with $\pi(X)$

• Decryption given a key $\pi$:
  – each letter $Y$ in the ciphertext $P$ is replaced with $\pi^{-1}(Y)$

Example:

$\begin{align*}
A & B C D E F G H I J K L M N O P Q R S T U V W X Y Z \\
\pi &= B A D C Z H W Y G O Q X S V T R N M L K J I P F E U \\
\text{BECAUSE} &\rightarrow \text{AZDBJSZ}
\end{align*}$
Strength of the General Substitution Cipher

- Exhaustive search is difficult
  - key space size is $26! \approx 4 \times 10^{26}$
- Dominates the art of secret writing throughout the first millennium A.D.
- Thought to be unbreakable by many back then
Cryptanalysis of Substitution Ciphers: Frequency Analysis

- Basic ideas:
  - Each language has certain features: frequency of letters, or of groups of two or more letters.
  - Substitution ciphers preserve the language features.
  - Substitution ciphers are vulnerable to frequency analysis attacks.
Frequency of Letters in English

CS426  Fall 2010/Lecture 2  15
Security Principles

• Security by obscurity doesn’t work

• Should assume that the adversary knows the algorithm; the only secret the adversary is assumed to not know is the key
Readings for This Lecture

Required readings:
- Cryptography on Wikipedia

Optional Readings:
- Security in Computing
  • Chapter 2: Basic Encryption and Decryption

Interesting reading
- The Code Book by Simon Singh
Coming Attractions …

- Cryptography: One-time Pad, Informational Theoretical Security, Stream Ciphers