Confidential Channels

Using encryption for network security
What is encryption?

- Encryption is used to achieve confidentiality
- Alice and Bob, wish to communicate secretly.
- Curious Carl wants to listen into their private chat.

As root, try: tcpdump -A -s0
Ciphers

• Ciphers operate to “garble” their input to make it unintelligible. The output of a cipher (ciphertext) does not bear any clear relation to the input (clear-text or plaintext).
  – The earliest recorded example of the use of a cipher is by Julius Caesar to his generals: He would shift each letter to the third letter following it in the alphabet.
    • Example: Attack now → Dwwdfn qrz
Assumptions about cipher design

• The adversary knows the cipher algorithm.
• To achieve secrecy, ciphers use keys.
• A key is an auxiliary input to the algorithm that must be kept private.
  – Only the key value is private. It is assumed that the enemy knows how keys are generated.
Example: Vigenere cipher

\[ K = \text{VECTOR} = (21, 4, 2, 19, 14, 17) \]

| W | E | W | I | L | L | M | E | E | T | A | T | M | I | D | N | I | G | H | T |
| 22| 4 | 22| 8 | 11| 11| 12| 4 | 4 | 19| 0 | 19| 12| 8 | 3 | 13| 8 | 6 | 7 | 19|
| 21| 4 | 2 | 19| 14| 17| 21| 4 | 2 | 19| 14| 17| 21| 4 | 2 | 19| 14| 17| 21| 4 |
|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 17| 8 | 24| 1 | 25| 2 | 7 | 8 | 6 | 12| 14| 10| 7 | 12| 5 | 6 | 22| 23| 2 | 23|
| R | I | Y | B | Z | C | H | I | G | M | O | K | H | M | F | G | W | X | C | X |
Breaking the Vigenere Cipher

• The probability distribution of characters
Looking at the example again

\[ K = \text{VECTOR} = (21, 4, 2, 19, 14, 17) \]
Index of coincidence

\[ c_i = \# \text{ of occurrences of the } i\text{-th character} \]

\[ c = \sum_i c_i \quad p_i = \frac{c_i}{c}, \]

\[ p_i = \text{frequency of the } i\text{-th character} \]

\[ IC = \sum_{i=0\ldots25} p_i^2 \]

\[ IC \text{ for random text } \approx 0.038 \]

\[ IC \text{ for typical English } \approx 0.065 \]
Choosing a cipher

- Ciphers are vulnerable to many known analysis techniques, and one must count on new attacks being discovered.

- General advice:
  - Avoid proprietary commercial ciphers whose design has not been publicly scrutinized. Do not develop your own if good alternatives exist: Adopt standards.
General encryption schemes
Symmetric vs. Asymmetric

• If the encryption and decryption keys are equal*, the scheme is said to be **symmetric**

• If the encryption and decryption keys differ, and moreover the decryption key cannot be computed from knowledge of the algorithm and encryption key, the scheme is **asymmetric**
Security of ciphers

From the Vigenere cipher to the Vernam one-time pad
Attacks on Encryption Schemes

• Types:
  – Passive:
    • Ciphertext only
    • Known-plaintext
  – Active:
    • Chosen plaintext (CPA)
    • Adaptive CPA
    • Chosen-ciphertext (CCA1)
    • Adaptive CCA (CCA2)

• Outcomes:
  – Total Break (key recovery)
  – Recovery of plaintext
  – Distinguishability between two alternative encrypted texts

• Most stringent security: IND-CCA2
Perfect cipher

- If the Vigenere cipher has key at least as long as the plaintext, is chosen at random, and used only once:
  - The scheme is called the **Vernam One-Time Pad**
  - It is provably unbreakable, even if the adversary has infinite computational power

- Reasoning: Given some ciphertext, any message of the same size would encrypt to the observed ciphertext under some key.
Perfect secrecy

- Shannon proved that the only cipher that is secure against an all-powerful adversary
  - Has key length equal to, or larger than the message
  - The key is random
  - Used only once
  - As inefficient as the Vernam one-time pad
Modern ciphers

• Operates on binary plaintext
• Uses binary keys of **fixed length**
• Different types of ciphers:
  – Public key/asymmetric ciphers
  – **Symmetric ciphers**
    • Stream ciphers (RC4, A5/x, Helix, SEAL)
    • Block ciphers (Triple-DES, Blowfish, AES)
Modern ciphers (continues)

• Two basic operations
  – Substitution: Substitutes a code symbol (for instance bit octets) for another.
    • Example: shifts (Vegenere cipher), xor
  – Permutation: Transposes or re-orders the symbols present in the code

• Both steps are needed for security