Internet Security

- **Q: What are the goals of attackers?**
  - From machines
    - *Infiltration*: take over machines/resources
      - *Defacement*: replace legitimate content
    - *Denial of service*
  - From users
    - Get data
      - Credit card, password, ...
    - Get traffic
      - Attention = money
      - The real currency of our age is user's attention
- **Q: How do attackers achieve the goal?**
  - Many, many different ways
    - *Phishing*: spoof web site to look like the real one
    - *Pharming* (*DNS cache poisoning*): wrong DNS resolution, for example
    - *Packet sniffing*
    - *Man-in-the-middle attack*
    - Password brute-force attack
    - *Buffer overflow*
    - *Client-state manipulation*: cookie poisoning
    - Cross-domain vulnerability
      - *Cross-site request forgery (XSRF)*
      - *Cross-site script inclusion (XSSI)*
      - *Cross-site scripting (XSS)*
    - *SQL injection*
  - Note: some of these vulnerabilities can be controlled by "good" programming practice. More discussion later
- **Q: When we communicate over Internet, what type of guarantee do we want?**
  - *Confidentiality*
  - *Message/data integrity*
  - *Authentication*

  - *Authorization*

- **Q: How can we keep confidentiality of the messages?**
  - *Steganography*: "embed" true message within harmless-looking message
    * Kathy is laughing loudly
    * Change the lowest bit of image pixels
    * "Security by obscurity"
  - *Encryption*: "scramble" message with a key, so that it wouldn't make sense to others unless they have the key
    * e.g., bitwise XOR with k

      11110000 (message) XOR 10111001 (key) -> 01001001 (ciphertext)

      01001001 (ciphertext) XOR 10111001 (key) -> 11110000 (message)

Symmetric Key Cryptography

- **[Encryption as generalization of XOR example]**

  In general, an encryption algorithm requires:
  - c = F(m, k): encryption function (m XOR k)
    * m: message = *plaintext*. want to keep secret
    * c: *ciphertext*. transmitted over insecure channel
  - m = F'(c, k): decryption function. inverse of F (c XOR k)
    * From above, m = F'(F(m, k), k)
    * e.g., ((m XOR 10111001) XOR 10111001) = m
  - F(m, k), F'(m, k) are called "cipher"

- **Q: What other property should F(m, k) have?**
  - Ideally, one should never be able to guess m from c alone
    * Ciphertext should not reveal any information about plaintext
  - *Perfect secrecy* (= *Shannon secrecy*)
    * For all plaintext x and ciphertext y, Pr(x | y) = Pr(x)

    * OTP (one time pad) encryption is proven to be perfectly secret, but due to practical limitation, cannot be used directly
    * Many encryption algorithms try to "mimic" OTP, e.g., RC4

- Commonly used ciphers
  - DES (data encryption standard)
    * 64 bit block cipher
    * Vulnerable to brute-force attack due to short key
      - Triple DES
  - AES (advanced encryption standard)
    * 128 bit block cipher
    * 128, 192, 256 bit keys
    * Adopted by NIST (national institute of standard and technology) as a replacement of DES in 2000
  - IDEA, A5 (used by GSM), ...

- [AES encryption animation]

  Remark:

  1. Addition and multiplication used for MixColumn step are slightly different from standard definition.
  2. MixColumn step "mixes" values from multiple bytes. Other steps do not mix values from multiple bytes.

- Key agreement problem
  - Q: How can we agree on a key "secretly" over the Internet?
    * Out-of-band communication?
  - Q: After A and B agreeing on secret key, how can we prevent B from impersonating A to C?
    * Q: n parties. How many keys?
  - Q: Want to keep communication confidential between every party. How many keys do we need for n parties?