Lecture 14 Outline

October 21, 2016

Reading: *text*, §10* **Assignments**: Homework 2, due Oct. 21; Lab 2, due Oct. 21

1. Greetings and felicitations!
2. Puzzle of the Day
3. Cryptography
   a. Codes vs. ciphers
   b. Attacks: ciphertext only, known plaintext, chosen plaintext
   c. Types: substitution, transposition
4. Classical Cryptography
   a. Monoalphabetic (simple substitution): $f(a) = a + k \bmod n$
   b. Example: Caesar with $k = 3$, RENAISSANCE → UHQDLVVDQFH
5. Symmetric Cryptography
   a. Monoalphabetic (simple substitution): $f(a) = a + k \bmod n$
   b. Example: Caesar with $k = 3$, RENAISSANCE → UHQDLVVDQFH
   c. Polyalphabetic: Vigenère, $f_i(a) = a + k_i \bmod n$
   d. Cryptanalysis: first do index of coincidence to see if it is monoalphabetic or polyalphabetic, then Kasiski method.
   e. Problem: eliminate periodicity of key
6. Long key generation
   a. Autokey cipher: key is keyword followed by plaintext or cipher text
   b. Running-key cipher: key is simply text; wedge is that (plaintext, key) letter pairs are not random (T/T, H/H, E/E, T/S, R/E, A/O, S/N, etc.)
   c. Perfect secrecy: when the probability of computing the plaintext message is the same whether or not you have the ciphertext; only cipher with perfect secrecy: one-time pads; C = `AZPR`; is that `DOIT` or `DONT`?
7. Product ciphers: DES, AES
8. Public-Key Cryptography
   a. Basic idea: 2 keys, one private, one public
   b. Cryptosystem must satisfy:
      i. Given public key, computationally infeasible to get private key;
      ii. Cipher withstands chosen plaintext attack;
      iii. Encryption, decryption computationally feasible (*note*: commutativity not required)
   c. Benefits: can give confidentiality or authentication or both
9. Use of public key cryptosystem
   a. Normally used as key interchange system to exchange secret keys (cheap)
   b. Then use secret key system (too expensive to use public key cryptosystem for this)
10. RSA
    a. Provides both authenticity and confidentiality
    b. Go through algorithm:
       Idea: $C = M^e \bmod n$, $M = C^d \bmod n$, with $ed \bmod \phi(n) = 1$
       Public key is (e, n); private key is d. Choose $n = pq$; then $\phi(n) = (p-1)(q-1)$.
    c. Example: $p = 5$, $q = 7$; then $n = 35$, $\phi(n) = (5-1)(7-1) = 24$. Pick $d = 11$. Then $ed \bmod \phi(n) = 1$, so $e = 11$
       To encipher 2, $C = M^e \bmod n = 2^{11} \bmod 35 = 2048 \bmod 35 = 18$, and $M = C^d \bmod n = 18^{11} \bmod 35 = 2$.
    d. Example: $p = 53$, $q = 61$; then $n = 3233$, $\phi(n) = (53-1)(61-1) = 3120$. Pick $d = 791$. Then $e = 71$
       To encipher M = `RENAISSANCE`, use the mapping `A = 00`, `B = 01`, ..., `Z = 25`, ␢ = 26.
       Then: M = `RE NA IS SA NC E␢` = 1704 1300 0818 1800 1302 0426
       So: $C = (1704)^{71} \bmod 3233 = 3106; \ldots = 3106\ 0100\ 0931\ 2691\ 1984\ 2927$