Lecture 17, May 8

Reading: §9.2–9.4 **Assignments due:** Homework #3, due May 13, 2013

Discussion Problem. The following is a passage from Sun Tsu's book *The Art of War*:[1]

> There are three ways in which a sovereign can bring misfortune upon his army:
> By commanding the army to advance or retreat, being ignorant of the fact that it cannot obey. This is called hobbling the army.
> By attempting to govern an army in the same way as he administers a kingdom, being ignorant if the conditions that obtain in an army. This causes restlessness in the soldiers' minds. Humanity and justice are the principles on which to govern a state, but not an army; opportunism and flexibility, on the other hand, are military rather than civic virtues.
> By employing the officers of his army without discrimination, through ignorance of the military principle of adaptation to circumstances. This shakes the confidence of the soldiers.

Does this apply to an organization with computers that are under attack, or are expected to be attacked? How?

Lecture outline.

1. Classical 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
2. Long key generation
   a. Autokey cipher:
      M = `THETREASUREISBURIED`
      K = `HELLOTHETREASUREISB`
      C = `ALPEFXHWNIIIKVLVQWE`
   b. Running-key cipher:
      M = `THETREASUREISBURIED`
      K = `THESECONDCIPHERISAN`
      C = `MOILVGOFXTMXZFLZAEQ`
      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
   d. Only cipher with perfect secrecy: one-time pads; C = `AZPR`; is that `DOIT` or `DONT`?
3. Product ciphers: DES, AES
4. 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
5. 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)

[1] Sun Tzu, *The Art of War*, Delta Publishing, New York, NY 10036 (1983) pp. 16–17