Lecture 17: May 5, 2021

Reading: *text*, §10.2–10.4

Assignments: Lab 2, due May 7, 2021 (Note new due date)
Homework 3, due May 10, 2021 (Note new due date)

1. Symmetric Cryptography
   (a) Polyalphabetic: Vigenère, $f_i(a) = a + k_i \bmod n$
   (b) Cryptanalysis: first do index of coincidence to see if it is monoalphabetic or polyalphabetic, then Kasiski method.
   (c) Problem: eliminate periodicity of key
2. 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?
3. Product ciphers
   (a) DES
   (b) 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)
6. El Gamal
   (a) Provides confidentiality; there is a corresponding algorithm for authenticity
   (b) Based on discrete log problem
7. RSA
   (a) Provides both authenticity and confidentiality
   (b) Based on difficulty of computing totient, $\phi(n)$, when n is difficult to factor
8. Elliptic curve cryptography
   (a) Works for any cryptosystem depending on discrete log problem
   (b) Example: Elliptic curve El Gamal
   (c) Selection of curves
9. Cryptographic Checksums
   (a) Function $y = h(x)$: easy to compute y given x; computationally infeasible to compute x given y
   (b) Variant: given x and y, computationally infeasible to find a second x' such that $y = h(x')$

   (c) Keyed vs. keyless

10. Digital Signatures
    (a) Judge can confirm, to the limits of technology, that claimed signer did sign message
    (b) RSA digital signatures: sign, then encipher, then sign