Lecture 8: Cryptography Part 2

Date: October 14, 2013 ***Homework Due***: Oct. 18 at 5:00pm

1. Perfect secrecy
   a. When having the ciphertext doesn't tell you anything about the plaintext
2. Classical cryptography
   a. Cæsar cipher; example, with key 'D' (3), RENAISSANCE → UHQDLVVDQFH
   b. Vigenère cipher; example: with key 'DAY', RENAISSANCE → UELDIQVALFE
   c. Problem: key is periodic; try to eliminate it
   d. Running-key cipher:
      K = `THESECONDCIPHERISAN`
      M = `THETREASUREISBURIED`
      C = `MOILVGOFXTMXZFLZAEQ`
   e. One-time pad; C = `AZPR`; is the key `XLHY` (`DOIT`) or `XLCY` (`DONT`)
   f. Data Encryption Standard
      i. Used in the triple-DES form now
   g. Advanced Encryption Standard
3. Use on a network
   a. Interchange key
   b. Session (data encryption) key
4. Public-Key Cryptography
   a. Basic idea: two keys, one public and one private, that are inverses
   b. Cryptosystem must satisfy:
      i. Given public key, computationally infeasible to get private key;
      ii. Cipher withstands chosen plaintext attack;
      iii. Encryption, decryption can be done quickly using a computer
   c. Benefits: can give confidentiality or authentication or both
   d. Use of public key cryptosystem
      i. Normally used as key interchange system to exchange secret keys (cheap)
      ii. Then use secret key system (too expensive to use public key cryptosystem for this)
   e. Common systems: RSA, El Gamal (encryption), Diffie-Hellman (authentication)
5. Digital signatures
   a. Idea: judge can confirm, to the limits of technology, that claimed signer did sign message
   b. Cryptographic checksum: math function easy to compute given input, very difficult to derive input from output
   c. Classical: use trusted third party
   d. Public key: encipher it using private key