

Notes for November 1, 1999

1. Greetings and Felicitations!
2. Puzzle of the Day
3. Public-Key Cryptography
 - a. Basic idea: 2 keys, one private, one public
 - b. Cryptosystem must satisfy:
 - i. given public key, CI 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
4. Use of PKC
 - a. Normally used as key interchange system to exchange secret keys (cheap)
 - b. Then use secret key system (too expensive to use PKC for this)
5. RSA
 - a. Provides both authenticity and confidentiality
 - b. Go through algorithm:

Idea: $C = M^e \bmod n$, $M = C^d \bmod n$, with $ed \bmod \phi(n) = 1$.

Proof: $M^{\phi(n)} \bmod n = 1$ [by Fermat's theorem as generalized by Euler]; follows immediately from $ed \bmod \phi(n) = 1$.

Public key is (e, n) ; private key is d . Choose $n = pq$; then $\phi(n) = (p-1)(q-1)$.
 - c. Example:

$p = 5$, $q = 7$; $n = 35$, $f(n) = (5-1)(7-1) = 24$. Pick $d = 11$. Then $de \bmod \phi(n) = 1$, so choose $e = 11$. 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: $p = 53$, $q = 61$, $n = 3233$, $f(n) = (53-1)(61-1) = 3120$. Take $d = 791$; then $e = 71$. Encipher $M =$ RENAISSANCE: A = 00, B = 01, ..., Z = 25, blank = 26. Then:
 $M =$ RE NA IS SA NC Eblank = 1704 1300 0818 1800 1302 0426
 $C = (1704)^{71} \bmod 3233 = 3106$; *etc.* = 3106 0100 0931 2691 1984 2927
6. Authentication:
 - a. validating client (user) identity
 - b. validating server (system) identity
 - c. validating both (mutual authentication)
7. Basis
 - a. What you know
 - b. What you have
 - c. What you are
8. Passwords
 - a. How UNIX does selection
 - b. Problem: common passwords; Go through Morris and Thompson ; Klein and mine, *etc.*
 - c. May be pass phrases: goal is to make search space as large as possible and distribution as uniform as possible
 - d. Other ways to force good password selection: random, pronounceable, computer-aided selection
 - e. Go through problems, approaches to each, *esp.* proactive