

Lecture 15 Outline

October 24, 2016

Reading: *text*, §10*, 11.1*–11.2*, 11.4*

Assignments: Homework 3, due Nov. 4; Lab 3, due Nov. 4

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, 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
4. 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)
5. RSA
 - a. Provides both authenticity and confidentiality
 - b. Go through algorithm:
Idea: $C = M^e \bmod n$, $M = C^d \bmod n$, with $ed \bmod \phi(n) = 1$
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 $M = \text{RENAISSANCE}$, use the mapping A = 00, B = 01, ..., Z = 25, $\emptyset = 26$.
Then: $M = \text{RE NA IS SA NC E}\emptyset = 1704\ 1300\ 0818\ 1800\ 1302\ 0426$
So: $C = (1704)^{71} \bmod 3233 = 3106; \dots = 3106\ 0100\ 0931\ 2691\ 1984\ 2927$
6. 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
7. Key Exchange
 - a. Needham-Schroeder and Kerberos
 - b. Public key; man-in-the-middle attacks
8. Key Generation
 - a. Cryptographically random numbers
 - b. Cryptographically pseudorandom numbers
 - c. Strong mixing function
9. Cryptographic Key Infrastructure
 - a. Certificates (X.509, PGP)
 - b. Certificate, key revocation
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