Lecture 13: October 23, 2019

Reading: *text*, §10.3–10.4

Assignments: Lab 2, due November 6, 2019
Homework 2, due October 21, 2019

1. Greetings and felicitations!
2. Puzzle of the Day
3. 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)
4. 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 $M =$ `RENAISSANCE`, use the mapping `A = 00`, `B = 01`, ..., `Z = 25`, b̸ = 26.
   Then: $M =$ `RE NA IS SA NC E`b̸ $= 1704\ 1300\ 0818\ 1800\ 1302\ 0426$
   So: $C = (1704)^{71} \bmod 3233 = 3106; \ldots = 3106\ 0100\ 0931\ 2691\ 1984\ 2927$
5. 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
6. 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