Outline for February 3, 2016

Reading: *text*, §10 handout; 10 in text

Assignments due: Homework 2, due February 5
Project progress report, due February 8

1. 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`, ƀ = 26.
      Then: $M =$ `RE NA IS SA NC Eƀ` $= 1704\ 1300\ 0818\ 1800\ 1302\ 0426$
      So: $C = (1704)^{71} \bmod 3233 = 3106; \ldots = 3106\ 0100\ 0931\ 2691\ 1984\ 2927$
2. Elliptic curve cryptography
   a. Elliptic curve is $y^2 = x^3 + ax + b \bmod p$, a, b, and p parameters; interested in points where x and y are integers (called *integer points*)
   b. Points P_1, P_2; define
      $$m = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & \text{when } P_1 \neq P_2 \\[2ex] \dfrac{3x_1^2 + a}{2y_1} & \text{otherwise.} \end{cases}$$
      Then sum $P_3 = (m^2 - x_1 - x_2, m(x_1 - x_3) - y_1)$
   c. Private key: k; public key, $Q = kP = P + \ldots + P$, adding P to itself k times
   d. Example: $y^2 = x^3 + 4x + 14 \bmod 2503$; take $P = (1002, 493)$
      Choose $k_{\text{Alice}} = 1379$ as private key, then public key $K_{\text{Alice}} = k_{\text{Alice}} P \bmod p = (1041, 1659)$
      Similarly, private key $k_{\text{Bob}} = 2001$ gives public key $K_{\text{Bob}} = (629, 548)$
      Then Alice computes $k_{\text{Alice}} K_{\text{Bob}} \bmod p = 1379(629, 548) \bmod 2503 = (2075, 2458)$
      And Bob computes $k_{\text{Bob}} K_{\text{Alice}} \bmod p = 2011(1041, 1659) \bmod 2503 = (2075, 2458)$
3. 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
4. Key exchange protocols