# Outline for May 11, 2004

1. Simple substitution ciphers
   a. Discuss breaking Vigenère (Kasiski method).
   b. Go through one-time pads
2. DES
   a. Product cipher with 64 bits in, 64 bits out, and 16 48-bit round keys generated from 56 bit key
   b. Note S-boxes are real heart of algorithm
   c. Differential cryptanalysis: first version unusable as at 16 rounds, more plaintext/ciphertext pairs needed than exhaustive key trial; but for 15 rounds, cuts this time. Later versions cut it to $2^{47}$ tries. Works by comparing xors of results with xors of corresponding plaintext. Designers of DES knew about this one, hence the design of the S-boxes
   d. Linear cryptanalysis drops required chosen plaintext/ciphertext pairs to $2^{42}$; not known to designers of DES.
   e. Triple DES and EDE mode
3. Public Key
   a. Requirements
      i. computationally easy to encipher, decipher
      ii. computationally infeasible to get private key from public
      iii. chosen plaintext attack computationally infeasible
   b. based on NP-hard problems (knapsack)
   c. based on hard mathematical problems (like factoring)
4. Do RSA
   a. Exponentiation cipher: $C = M^e \bmod n$, $M = C^d \bmod n$; $d$ is private key, $(e, n)$ is public key; must choose $d$ first, then $e$ so that $ed \bmod \phi(n) = 1$.
   b. Example: $p = 5$, $q = 7$, $n = 35$, $\phi(n) = 24$; choose $e = 11$, then $d = 11$. HELLO WORLD is 07 04 11 11 14 22 14 17 11 03; enciphering is $C = 07^{11} \bmod 35 = 28$, *etc*. so encipherment is 28 09 16 16 14 08 14 33 16 12.
   c. Problems: rearrangement of blocks (“is the attack on?” NO vs. ON); precomputation of possible answers
5. Cryptographic checksums
   a. Requirements
   b. Keyed vs. keyless cryptographic checksums
   c. HMAC