Outline for April 25, 2000

1. What is a cryptosystem?
   a. $(\mathcal{M}, \mathcal{C}, \mathcal{K}, \mathcal{D}, \mathcal{E})$
   b. attacks: known ciphertext, known plaintext, chosen plaintext
2. Transposition ciphers
   a. Show rail-fence cipher as example
   b. Show anagramming
3. Simple substitution ciphers
   a. Do Cæsar cipher
   b. Present Vigenère tableau
   c. Discuss breaking it (Kasiski method).
   d. Go through one-time pads
4. 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. Complementation property: $\mathrm{DES}_k(m) = (\mathrm{DES}_{k'}(m'))'$ where x' is the bitwise complement of x;
   d. 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
   e. Linear cryptanalysis drops required chosen plaintext/ciphertext pairs to 2^{42}; not known to designers of DES.
   f. Triple DES and EDE mode
5. Public Key
   a. based on NP-hard problems (knapsack)
   b. based on hard mathematical problems (like factoring)
6. 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. Why? as $ed \bmod \phi(n) = 1$, $ed = t\phi(n) + 1$ for some integer t. Then

$$
\begin{aligned}
C^d \bmod n &= (M^e \bmod n)^d \bmod n \\
&= M^{ed} \bmod n \\
&= M^{t\phi(n)+1} \bmod n \\
&= M(M^{t\phi(n)} \bmod n) \bmod n \\
&= \mathrm{M}(M^{\phi(n)} \bmod n)^t \bmod n \\
&= M(1)^t \bmod n \\
&= M \bmod n
\end{aligned}
$$

   by Fermat's Little Theorem
   c. 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.