Outline for April 9, 1997

1. Greetings and Felicitations
   a. For NTU: All homework is due 1 week after the due date; I'll put this explicitly on future assignments
2. Solving ax mod n = 1:
   a. { r_1, ..., $r_{\mathrm{PHI}(n)}$} reduced set of residues
   b. by definition, { ar_1 mod n, ..., $ar_{\mathrm{PHI}(n)}$ mod n} is same set
   c. So, $\prod (ar_i \bmod n) = \prod r_i$ (upper bound PHI(n)
   d. ($a^{\mathrm{PHI}(n)}$ mod n) $\prod r_i = \prod r_i$, giving $a^{\mathrm{PHI}(n)}$ mod n = 1.
   e. Ex: a = 5, n = 7; 5x mod 7 = 1; x = $5^{\mathrm{PHI}(7)-1}$ mod 7 = 5^5 mod 7 = 3.
3. Euclid's extended GCD algorithm
   a. GCD(4, 6): remainder of 4 into 6 is 2; remainder of 2 into 4 is 0; GCD is 2
   b. GCD(14, 22): remainder of 14 into 22 is 8; remainder of 8 into 14 is 6; remainder of 6 into 8 is 2; remainder of 2 into 6 is 0; GCD is 2
   c. Extend: find x, y s.t. xa + yn = gcd(a, n) as then if GCD is 1, xa +yn = 1 and x solves ax mod n = 1.
   d. Ex. 1: a = 5, n = 7
      $g_0 = 7$, $x_0 = 0$, $y_0 = 1$ (note $g_0 = 5x_0 + 7y_0$);
      $g_1 = 5$, $x_1 = 1$, $y_1 = 0$ (note $g_1 = 5x_1 + 7y_1$); $q = g_0/g_1 = 1$
      $g_2 = 2 = 7 - 5q$; $x_2 = 0 - 1q = -1$; $y_2 = 1 - 0q = 1$ (note $g_2 = 5x_2 + 7y_2$); $q = g_1/g_2 = 2$;
      $g_3 = 1 = 5 - 2q$; $x_3 = 1 - (-1)2 = 3$; $y_3 = 0 - (1)2 = -2$ (note $g_3 = 5x_3 + 7y_3$); $q = g_2/g_3 = 0$
      GCD is x_3, or 3.
   e. Hence 5x mod 7 = 1 => x = 3, and 5(3) + 7(-2) = 15 - 14 = 1
4. ax mod n = b
   a. Solve ax_0 mod n = 1, then x = bx_0 mod n
   b. Ex: 5x mod 7 = 3; as x_0 = 3, x = 3(3) mod 7 = 2
5. Chinese Remainder Theorem
   a. Let g = gcd(a, n) and g divide b. Then ax mod n = b has g solutions of the form x = [(b/g)x_0 + t(n/g)] mod n, where x_0 solves (a/g)x mod (n/g) = 1.
   b. Ex: solve 5x mod 21 = 1. 21 = 3(7); need x_1, x_2 such that
      $5x_1$ mod 3 = 1 and $5x_2$ mod 7 = 1; solns. x_1 = 2, x_2 = 3. So the solution to x mod 3 = 2 and x mod 7 = 3 also solves 5x mod 21 = 1
      Technique: find y_1: (21/3)y_1 mod 3 = 1, so 7y_1 mod 3 = 1, or y_1 = 1
      find y_2: (21/7)y_2 mod 7 = 1, so 3y_2 mod 7 = 1, or y_2 = 5
      x = [(21/3)y_1x_1 + (21/7)y_2x_2] mod 21 = ((7)(1)(2) = (3)(5)(3)) mod 21 = 59 mod 21 = 17
6. Transposition ciphers
   a. Show rail-fence cipher as example
   b. Show anagramming