Outline for January 12, 1999

1. Measures of strength
   a. unconditionally secure (theoretically unbreakable)
   b. conditionally secure (unbreakable in practise); note environment often affects this
   c. weak (breakable)
2. Quote for the Day
3. How to measure strength: Entropy
   a. Given C, how much uncertainty in m?
   b. attacker wants 0
   c. sender wants $lg(n)$, n = length of message
4. Requirements for function $H(p_1, \ldots, p_n)$; explain these
   a. Review probability notation; assume $p_1 + \ldots + p_n = 1$.
   b. $H(p_1, \ldots, p_n)$ max when $p_1 = \ldots = p_n = 1/n$
   c. For permutation π of $(1, \ldots, n)$, $H(p_{\pi(1)}, \ldots, p_{\pi(n)}) = H(p_1, \ldots, p_n)$
   d. $H(p_1, \ldots, p_n) \geq 0$; it is 0 if all p_i are 0 except for one, which is 1
   e. $H(p_1, \ldots, p_n, 0) = H(p_1, \ldots, p_n)$
   f. $H(1/n, \ldots, 1/n) \leq H(1/(n+1), \ldots, 1/(n+1))$
   g. $H(1/mn, \ldots, 1/mn) = H(1/n, \ldots, 1/n) + H(1/m, \ldots, 1/m)$
   h. H continuous for its arguments [mention if time]
   i. $p = \Sigma p_i$, $q = \Sigma q_i$, $p > 0$, $q > 0$, $p + q = 1$ implies
      $H(p_1, \ldots, p_m, q_1, \ldots, q_n) = H(p, q) + pH(p_1/p, \ldots, p_m/p) + qH(q_1/q, \ldots, q_n/q)$ [mention if time]
   j. Only function which does this is $H(p_1, \ldots, p_n) = -\lambda\Sigma_k p_k\, lg(p_k)$
5. Examples
   a. rate for message of length n is $r = H(\mathbf{X})/n$; for English, 1 to 1.5
   b. absolute rate: assume all chars are equally likely; assuming L chars, $R = lg\ L$; for English, 4.7
   c. redundency $D = R - r$; for English, 3.2 to 3.7
6. Equivocation
   a. Given some info, how much uncertainty is left
   b. Ex: 8 bit integer, => $H(\mathbf{X}) = 8$; parity bit 0 => $H(\mathbf{X}|\mathbf{Y}) = 7$ (work it out)
   c. $H(\mathbf{X}|\mathbf{Y}) = -\Sigma_{\mathbf{x},\mathbf{y}} p(\mathbf{X},\mathbf{Y})\ lg(p(\mathbf{X}|\mathbf{Y}))$
   d. As $p(\mathbf{X},\mathbf{Y}) = p(\mathbf{X}|\mathbf{Y})p(\mathbf{Y})$, $H(\mathbf{X}|\mathbf{Y}) = -\Sigma_{\mathbf{y}} p(\mathbf{Y})\Sigma_{\mathbf{x}} p(\mathbf{X}|\mathbf{Y})\ lg(p(\mathbf{X}|\mathbf{Y}))$ [joint probability]
7. More examples
   a. Throw die, flip coin; $p(\mathbf{X}=3, \mathbf{Y}=\text{H}) = 1/12 = p(\mathbf{X}=3)p(\mathbf{Y}=\text{H})$ [independence]
   b. Toss coin; if heads, 3-sided die; if tails, 6-sided die. Prob. result is 3?
      $p(\mathbf{Y}=\text{H}, \mathbf{X}=3) = p(\mathbf{X}=3|\mathbf{Y}=\text{H})p(\mathbf{Y}=\text{H})$ *etc.*
   c. like b, but prob. result is 4:
      $p(\mathbf{Y}=\text{H}, \mathbf{X}=4) = p(\mathbf{X}=4|\mathbf{Y}=\text{H})p(\mathbf{Y}=\text{H})$ *etc.*
8. Uncertainty in above
   a. $H(\mathbf{X}|\mathbf{Y}) = lg\ 6 = H(\mathbf{X})$ [independence; as $p(\mathbf{X}|\mathbf{Y}) = p(\mathbf{X})$ and $\Sigma_{\mathbf{y}} p(\mathbf{Y}) = 1$]
   b. $H(\mathbf{X}|\mathbf{Y}) = (1/2)[lg\ 3 + lg\ 6] = (1/2)\ lg\ 18$
9. Perfect Secrecy
   a. $H(\mathbf{M}|\mathbf{C}) = H(\mathbf{M})$ or $p(\mathbf{M}|\mathbf{C}) = p(\mathbf{M})$
   b. $H(\mathbf{C}|\mathbf{M}) = H(\mathbf{C})$ or $p(\mathbf{C}|\mathbf{M}) = p(\mathbf{C})$ [same thing]

10. Unicity distance
    a. given C, what is uncertainty in K?
    b. KHOOR ZRUOG; unicity distance is 0 ($k = 23$)
    c. J; uncity distance is 1 as it's K=25 (I) or K=9 (A)
    d. Smallest N for which $H(\mathbf{K}|\mathbf{C}) \approx 0$ is amount of ciphertext needed to uniquely determine key
    e. "unconditionally secure" if no such N exists
    f. Can show: $N = H(\mathbf{K})/D \Rightarrow H(\mathbf{K}) - DN = 0$
    g. if number of keys = number of meaningful messages, $H(\mathbf{K}) = RN$, so
       $H(\mathbf{K}) - DN = RN - DN = (R - D) N = rN \neq 0$
11. Random cipher
    a. For a given K, C, $D_K(C)$ equally likey to produce any (meaningless or meaningful) message
12. Transposition ciphers
    a. Show rail-fence cipher as example
    b. Show anagramming
13. Simple substitution ciphers
    a. Do Cæsar cipher
    b. Go through how to break it
    c. Present Vigenère tableau
    d. Discuss breaking it (Kasiski method). Note index of coincidence is probability 2 letters chosen at random from ciphertext are alike
    e. Generalize to very long keys and show running key and autokey
    f. Go through rotor systems (Enigma)
    g. Go through one-time pads
14. Polygram substitution cipher: Playfair
    a. Key is 5 by 5 grid
    b. If m_1, m_2 in same row, c_1, c_2 are to immediate right of m_1, m_2 respectively
    c. If m_1, m_2 in same column, c_1, c_2 are below m_1, m_2
    d. If $m_1 = m_2$, insert null in text
    e. if m_1, m_2 in different rows and columns, c_1, c_2 form rectangle with c_1 in m_1's row and c_2 in m_2's row
    f. if odd number of characters in message, append null.

Quote

"Without harmony in the state, no military expedition can be undertaken; without harmony in the army, no battle array can be formed."
— Sun Tzu, *The Art of War*, (Translated by James Clavell), Dell Publishing, New York, NY 10036 (1983).