a. rate for message of length n is $r = H(X)/n$; 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

Outline for April 2, 1997

1. Greetings and Felicitations
   a. Please speak into the microphone
2. What is cryptography?
   a. cipher v. code
   b. plaintext (cleartext) M, ciphertext C, key k
   c. encryption Ek, decryption Dk
3. Requirements for a cryptosystem
   a. enciphering, deciphering is efficient for all keys
   b. easy to use
   c. strength is depends on secrecy of keys *only*, not on secrecy of E or D
4. What it can do: Secrecy
   a. c.i. to determine Dk from C even if corresponding M known
   b. c.i. to determine M from C if k unknown
5. What it can do: Data Authenticity (Integrity)
   a. c.i. to determine Ek from C even if corresponding M known
   b. c.i. to find a C' such that Dk(C') is valid plaintext
6. Attacks
   a. ciphertext only
   b. known plaintext
   c. chosen plaintext
   d. chosen ciphertext
7. Measures of strength
   a. unconditionally secure (theoretically unbreakable)
   b. conditionally secure (unbreakable in practise); note environment often affects this
   c. weak (breakable)
8. 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
9. Requirements for function H(p1, …, pn); explain these
   a. Review probability notation; assume p1 + … + pn = 1.
   b. H(p1, …, pn) max when p1 = … = pn = 1/n
   c. For permutation π of (1, …, n), H(pπ(1), …, pπ(n)) = H(p1, …, pn)
   d. H(p1, …, pn) $\geq$ 0; it is 0 if all pi are 0 except for one, which is 1
   e. H(p1, …, pn, 0) = H(p1, …, pn)
   f. H(1/n, …, 1/n) $\leq$ H(1/(n+1), …, 1/(n+1))
   g. H(1/mn, …, 1/mn) = H(1/n, …, 1/n) + H(1/m, …, 1/m)
   h. H continuous for its arguments [mention if time]
   i. p = Σpi, q = Σqi, p > 0, q > 0, p + q = 1 implies
      H(p1, …, pm, q1, …, qn) = H(p, q) + pH(p1/p, …, pm/p) + qH(q1/q, …, qn/q) [mention if time]
   j. Only function which does this is H(p1, …, pn) = $-\lambda\Sigma_k p_k \lg(p_k)$
10. Examples