14. Attacks
    a. ciphertext only
    b. known plaintext
    c. chosen plaintext
    d. chosen ciphertext

Quote

"All warfare is based on deception. Hence, when able to attack, we must seem unable; when using our forces, we must seem inactive; when we are near, we must make the enemy believe we are far away; when far away, we must make him believe we are near. Hold out baits to entice the enemy. Feign disorder, and crush him. If he is secure at all points, be prepared for him. If he is in superior strength, evade him. If your opponent is of choleric temper, seek to irritate him. Pretend to be weak, that he may grow arrogant. If he is taking his ease, give him no rest. If his forces are united, separate them. Attack him where he is unprepared, appear where you are not expected."
— Sun Tzu, *The Art of War*, (Translated by James Clavell), Dell Publishing, New York, NY 10036 (1983).

Outline for January 7, 1999

1. Greetings and Felicitations
   a. Review general information
2. Quote of the Day
3. Basic components
   a. Confidentiality
   b. Integrity
   c. Availability
4. Threats
   a. snooping
   b. modification
   c. masquerading; contrast with delegation
   d. repudiation of origin
   e. denial of receipt
   f. delay
   g. denial of service
5. Role of policy
   a. example of student copying files from another
   b. emphasize: policy *defines* security
   c. distinguish between policy and mechanism
6. Goals of security
   a. prevention
   b. detection
   c. recovery
7. Trust
   a. hammer this home: all security rests on trust
   b. first problem: security mechanisms correctly implement security policy; walk through example of a program that logs you in; point out what is trusted
   c. second problem: policy does what you want; define secure, precise
8. Operational issues; change over time
   a. cost-benefit analysis
   b. risk analysis (comes into play in cost-benefit too)
   c. laws and customs
9. Human Factors
   a. organizational problems
   b. people problems (include social engineering)
10. What is cryptography?
    a. cipher *vs.* code
    b. plaintext (cleartext) M, ciphertext C, key k
    c. encryption E_k, decryption D_k
11. 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
12. What it can do: Secrecy
    a. computationally infeasible to determine D_k from C even if corresponding M known
    b. computationally infeasible to determine M from C if k unknown
13. What it can do: Data Authenticity (Integrity)
    a. computationally infeasible to determine E_k from C even if corresponding M known
    b. computationally infeasible to find a C' such that $D_k(C')$ is valid plaintext