Outline for November 3, 2003

Reading: Chapters 12.3–12.6

Discussion Problem
The PGP secure mailing system uses both RSA and a classical cipher called IDEA. When one installs PGP, the software generates two large (512 bits or so) numbers, to produce a modulus of 1024 bits. Such a number is too large to be factored easily. The private and public keys are generated from these quantities. The private key is enciphered with a classical cipher using a user-supplied pass phrase as the key. To send a message, a 128-bit key is randomly generated, and the message enciphered using IDEA with that key; the key is enciphered using the recipient’s public key, and the message and enciphered key are sent.

1. If you needed to compromise a user’s PGP private key, what approaches would you take?
2. It’s often said that PGP gets you the security of a key with length 1024. Do you agree?

Outline for the Day

1. Challenge-response systems
   a. Computer issues challenge, user presents response to verify secret information known/item possessed
   b. Pass-algorithms
   c. One-time passwords (example: S/Key)
   d. Hardware: token/calculator, time card
   e. Attack: dictionary search for $k$ given challenge $r$, response $E_k(r)$
   f. Defense: encipher random challenges
2. Biometrics
   a. Depend on physical characteristics
   b. Examples: pattern of typing (remarkably effective), retinal scans, etc.
3. Location
   a. Bind user to some location detection device (human, GPS)
   b. Authenticate by location of the device
4. Combinations
   a. PAM