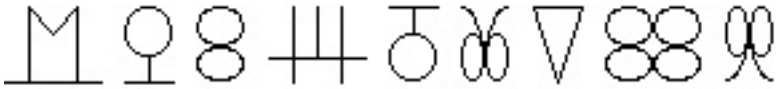
Lecture 21, May 17

Reading: §10.4, 10.6, 11.3, 11.4.1, 12

Assignments due: Project Teams, due May 20, 2013 at 11:55pm
Homework #4, due May 24, 2013 at 11:55pm

Discussion Problem. Analyzing a cipher requires being able to spot patterns. See how good you are. What is the pattern in the following?



Lecture outline.

1. Project information
2. Cryptographic Key Infrastructure
   a. Certificates (X.509, PGP)
   b. Certificate, key revocation
3. Digital Signatures
   a. Judge can confirm, to the limits of technology, that claimed signer did sign message
   b. RSA digital signatures: sign, then encipher
4. Networks and ciphers
   a. Where to put the encryption
   b. Link vs. end-to-end
5. PEM, PGP
   a. Goals: confidentiality, authentication, integrity, non-repudiation (maybe)
   b. Design goals: drop in (not change), works with any RFC 821-conforment MTA and any UA, and exchange messages without prior interaction
   c. Use of Data Exchange Key, Interchange Key
   d. Review of how to do confidentiality, authentication, integrity with public key IKs
6. Authentication
   a. validating client (user) identity
   b. validating server (system) identity
   c. validating both (mutual authentication)
7. Basis: what you know/have/are, where you are
8. Passwords
   a. Problem: common passwords
   b. May be pass phrases: goal is to make search space as large as possible, distribution as uniform as possible
   c. Other ways to force good password selection: random, pronounceable, computer-aided selection
9. Password Storage
   a. In the clear; Multics story
   b. Enciphered; key must be kept available
   c. Hashed; show UNIX versions, including salt