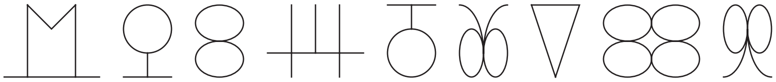
Outline for November 14, 2003

Reading: Chapters 15.2.2, 16.1, 16.3

Discussion Problem

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



Outline for the Day

1. Privilege in Languages
    a. Nesting program units
    b. Temporary upgrading of privileges
2. Information Flow
    a. What is it?
    b. Entropy-based analysis: flows from x to y if $H(x_s|y_t) < H(x_s|y_s)$ where system starts in state s, transitions to state t
    c. Examples: $y := x$, $x := y + z$, **if** $x = 1$ **then** $y := 0$ **else** $y := 1$
3. Compiler-Based Mechanisms
    a. Labels on variables; all examples use Bell-LaPadula style labels
        i. Review lub(X, Y), glb(X, Y)
    b. Certifying sets of statements
    c. Declarations
    d. Assignments
    e. Compound statements
    f. Conditional statements
    g. Iterative statements