Date: Thu, 14 Sep 1995 14:29:57 EDT

CLASSICAL CRYPTOGRAPHY COURSE
BY LANAKI
September 14, 1995

OUTLINE

LECTURE 1 - SIMPLE SUBSTITUTION

1. Intro - First Principles - Global Mathematical Nature
2. Keyword Systems and Conventions Used
3. Simple Substitution Cryptanalysis without/with Complexities

   a. Eyeball
   b. Frequency Distributions - General Nature of English Letters - Relationship to XENOS:French and German Solutions
   c. Friedman Techniques - Random vs Expected - Spaces and a Wealth of Tables: Digram, Trigram, and more
   d. C. C. Foster Techniques
   e. S-Tuck Techniques
   f. Pattern Words
   g. ELCY : Consonant Line Attack
   h. Sinkov Techniques
   i. Barker's Vowel Separation
   j. Non Pattern Words: MICROPOD/CODEX/ZYZZ "Dooseys"
   k. CM References for Risties
   l. SI SI Patterns
   m. Computer Program Aids - TEA Database, CDB, ABACUS, Computer Supplement
   n. References for More Material

4. Homework Problems

5. Variant Substitution Systems

SPECIAL CLASS ASSIGNMENT

Each student will pick his/her ONE favorite cipher from "The Cryptogram" for intensive study. Plan on researching the origin and history, use, methodology and "cracking" techniques. Be prepared to present and discuss with your classmates when we cover it in class. Be sure to include available computer programs and appropriate references.

My best to all,

LANAKI