Cryptography at The University of South Carolina

Douglas B. Meade

meade@math.sc.edu

http://www.math.sc.edu/~meade/

Cryptography as an application in …

- Number Theory (MATH 580)
  - Course homepage: http://www.math.sc.edu/~sumner/numbertheory/mainpage/math580.html
  - RSA Encryption Algorithm

    http://www.math.sc.edu/~sumner/numbertheory/rsa/encrypt.html

- (Numerical) Linear Algebra (MATH 526)
  - Course homepage:

    http://www.math.sc.edu/~meade/math526-F05/
  - Hill Substitution Cypher http://beta.mapleprimes.com/files/178_HillSubstCipher.mw

Cryptography as its own course

- Cryptography
  - Cross-listed as CSCE 557 and MATH 587
  - Course homepage: http://www.cse.sc.edu/~buell/csce557/csce557_2005_4fall.html
  - Syllabus: http://www.cse.sc.edu/syllabus/CSCE557.pdf

Cross-listing between CSCE & MATH

- Computer science/engineering students …
  - see relevant and interesting applications of mathematics
  - learn some new mathematics
  - motivated to take more mathematics courses

Cross-listing between CSCE & MATH

- Mathematics students …
  - see cutting-edge application of mathematics
  - appreciate importance of computational mathematics
  - exposed to practical issues related to implementing mathematics (Gnu MultiPrecision library)
  - motivated to take more computer science courses

Hill Substitution Cypher

- Reference:
  Linear Algebra and Its Applications,
  David C. Lay, Addison-Wesley, updated 3rd edition, 2006.

- Case Study (electronic supplement)

  http://www.math.sc.edu/~meade/math526-F05/misc/hillcipher.pdf

Hill Substitution Cypher

- Preparation

1. Specify alphabet and cypher/decypher array
   p = # characters in alphabet

2. Select key matrix M
   invertible mod p: det M <> = mod p

3. Compute inverse key matrix
   M^{-1} M = I mod p

4. Share cypher/decypher array and M^{-1}

Hill Substitution Cypher

- Encryption

1. Convert message to numeric code
   + vectorize

2. Encode using key matrix
   e = Mv mod p

3. Convert numeric vector to string in alphabet

Hill Substitution Cypher

- Decryption

1. Convert encoded string to numeric code + vectorize

2. Decode using inverse key matrix
   $v = M^{-1}e \bmod p$

3. Convert numeric vector to string in alphabet

Hill Substitution Cypher

- Implementation
  - Maple
    - supports modular linear algebra
    - embedded components eliminate need to know any Maple to use [worksheet] [MapleNet]
  - MATLAB
    - does not support modular linear algebra