

Mathematics of Coding and Cryptography Worksheet 1

A substitution cipher replaces each occurrence of a particular letter with another prescribed letter. A substitution cipher is an example of a symmetric algorithm (why?) with $26!$ keys. An example of a key is

DEWTYNGHJOLKBXMPQZRAICSVU,

where for instance, each occurrence of the letter A would be replaced with a D, each B would be replaced with an E, and so on.

1. Using the included chart of relative letter frequency in the English language, try and decipher the following message encrypted with a simple substitution cipher.

DREC EC HUD DRA GEHT UV YLXIYEHDYHLA DRYD SN. BYMUSYN
EC SUCD EHLMEHAT DU BIN CIA; RA FUI MT PA LUH DAHD DU ACDYP-
MECR DRA CESBMELEDO UV Y TENALD BROCELYM NAM YDEUHC REB
PADFAAH SYH YHT LRAACA. PID CEHLA EH BMYLA UV DRA LRAA-
CAC RA CAAC HYSAC UV LRAACAC, LUHLABDC UV LRAACAC, SAY-
HEHKC UV LRAACAC, RECDUNEAC UV LRAACAC, LUHDAQDC UV
LRAACAC, BCOLRUMUKEAC UV LRAACAC, FRAH RA TUAC HUD
CU SILR GHUF YC CAHCA DRYD PAREHT AYLR UV DRACA LRAA-
CAC DRANA EC YMM DRYD, DRAH REC NAM YDEUHC REB PALUSAC
JANO LUSBMELYDAT.

The following website might help

<http://snicker.nebrwesleyan.edu/~mcclung/ciphers.php>

2. A permutation matrix is a square matrix with 0 or 1 entries, such that every row and column contains exactly one 1. An example of a 4×4 permutation matrix is

$$M = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

A permutation matrix is so named because it permutes the order of the standard basis vectors. (Recall that the n th standard basis vector \mathbf{e}_n is the vector whose entries are all 0 except the n th entry which is a 1). That is $M\mathbf{e}_n = \mathbf{e}_m$ for some m .

- (a) Relate the structure of the permutation of the standard basis vectors to the structure of the permutation matrix. (i.e. how does the location of the 1s in the permutation matrix tell you how the standard basis vectors are going to be reordered?) I want a general answer, not just for the matrix M above.
- (b) If we have a 26×26 matrix, and we identify letters with the standard basis vectors (for instance $A = \mathbf{e}_1, B = \mathbf{e}_2$ and so on), then the permutation matrix determines a substitution cipher. How?

- (c) How would you represent the plain text of a message using this identification?
 - (d) How would you represent the cipher text?
 - (e) What is the significance of the inverse of such a permutation matrix in the context of the substitution cipher?
 - (f) Is there an easy way to find the inverse of such a permutation matrix?
 - (g) What is the significance of the intersection of the eigenspace associated to the eigenvalue $\lambda = 1$ and the standard basis vectors? What does this tell you about the key?
3. Suppose Eve's computing ability is increasing in time so that the (approximate) number of keys she can test per second at time t , is given by

$$n(t) = 2^{2(t+15)}$$

where t is measured in years (or fractions thereof). Suppose you have a 64 bit key (That is there are 2^{64} possible keys). Approximately how long will it take Eve to try every key, assuming she starts at $t = 0$?