

CIS 400/628

Homework #1

Spring 2005

1. Decrypt the following message. Produce a frequency count for each symbol.

U O F V T J < F J J L O F U J < < C J V
J V T J A O U L F < U > A O U > J N K
> U O U J V O N O F L A J L U < F > O
L N O U < J F O U J V A J > O U N > J
A J > O C J L O U J V O N > J L J V L <
O L N > J J A J L O U U O O N > J L J N
< F O O U O O A U L C > J F A O V U F >
V J < A J F L O J V L > V O O V L F > V
J < V > U < O O O F V T V O O J L > J U
> C A N U O F V T J < F J J L O F U J <
< C J V J V T J A O U L F < U > A O U
> J N < > U O U J V O N O U J L F L U J
< < < J J L > O U O F V T J < F J J L O
N > J L J V L U O J < F J J L O N > J L
J V L U O N > J L J V L U O C F L A J <
< > O N > J J < J J L U F L U J < < < J
J L > O U O F V T J < F J J L O N > J L
J V L U O J < F J J L O N > J L J V L U
O J < F J J L O C F L A J < < > O N > J
J < J J L U U J U > J L L N O C J V U F
V T O J J > V E J O O O C J > A A F U U
> V T U O F V T J < F J J L O > V N F U
L J < O < F O O J J J > V U O U A < O J
T J O J O L > J J U

The following four questions are taken from the Lewand book. I reproduce them here in case you do not have the book yet.

2. (Lewand, Exercises 1.3, #4) Prove that any two consecutive integers are relatively prime. Is the same true for any two consecutive odd integers? What about any two consecutive even integers?
3. (Lewand, Exercises 1.4, #7) For any integer x , prove that either $x^2 \equiv 0 \pmod{4}$ or $x^2 \equiv 1 \pmod{4}$.
4. (Lewand, Exercises 1.5, #3) Consider the message delivered by the Marquis de Lafayette to the Constituent Assembly on February 20, 1790:

“When the government violates the people’s rights, insurrection is, for the people and for each portion of the people, the most sacred of the rights and the most indispensable of duties.”

Ignoring punctuation and capitalization, encipher Lafayette’s message using:

- (a) An additive cipher with key = 16.
 - (b) A multiplicative cipher with key = 17.
 - (c) An affine cipher with additive key = 24 and multiplicative key = 3.
 - (d) A keyword cipher with keyword *constitution* and key letter = m.
5. (Lewand, Exercises 1.6, # 7) Write a program that accepts a text message [on stdin is permissible –sjc] and outputs the frequency of each letter appearing in the message.
- Do the optional part of this question as well: A bit more challenging (perhaps) would be to write a program that outputs the frequency of all *digraphs* in the message.