ECE 471/571: In Class Problem #1

Cryptanalysis of the Substitution Cipher

Electrical and Computer Engineering, University of Arizona,
Ming Li

1 Cryptanalysis of the Substitution Cipher

Determine the plaintext given that the following ciphertext was generated using the Substitution Cipher. Hint: F decrypts to w, and G to a.

EMGLOSUDCGDNCUSWYSFHNSFCYKDPUMLWGYICOXYSIPJCKQPKUGKMGOLICGI
NCGACKSNISACYKZSCKXECJCKSHYSXCGOIDPKZCNKSHICGIWYGKKGKGOLDSILKGOIU
SIGLEDSPWZUGFZCCNDGYYSFUSZCNXEOJNCGYEOWEUPXEZGACGNFGLKNSACIGOIYCKXC
JUCIUZCFZCCNDGYYSFEUEKUZCSOCFZCCNCIACZEJNCSHFZEJZEGMXCYHCJUMGKUCY

You are given the probability of occurrence of each of the 26 letters (rank: E T A O I N S H R D L ...)

Table 1. Probabilities of occurence of the 26 alphabets

A	B	C	D	E	F	G	H	I	J	K	L	M
0.082	0.015	0.028	0.043	0.127	0.022	0.020	0.061	0.070	0.002	0.008	0.040	0.024
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0.067	0.075	0.019	0.001	0.060	0.063	0.091	0.028	0.010	0.023	0.001	0.020	0.001

The most common digrams in English text:

TH, HE, IN, ER, AN, RE, ED, ON, ES, ST, EN, AT, TO, NT, HA, ND, OU, EA, NG, AS, OR, TI, IS, ET, IT, AR, TE, SE, HI, OF

and the most common trigrams in English text:

THE, ING, AND, HER, ERE, ENT, THA, NTH, WAS, ETH, FOR, DTH

Frequencies of each letter in the ciphertext:

Table 2. Letter occurences in the ciphertext

C	G	S	K	I	Y	U	N	Z	O	E
32	22	19	17	14	13	12	12	10	10	9

Frequent digrams in the ciphertext: ZC CN CG YS SF FZ GY

Helpful tool: http://https://www.cryptoclub.org/#vAllTools

Solution: the ciphertext-plaintext letter mapping is as follows (complete the rest by yourself):

Table 3. The ciphertext-plaintext letter mapping (selected).

C	G	S	K	I	Y	U	N	Z	O	E	F	D	M
e	a	o	s	d	r	t	l	h	n	i	w	b	m

The plaintext is from "The Diary of Samuel Marchbanks", by Robertson Davies, Clarke Irwin, 1947.

I may not be able to grow flowers, but my garden produces just as many dead leaves, old overshoes, pieces of rope, and bushels of dead grass as anybody's, and today I bought a wheelbarrow to help in clearing it up. I have always loved and respected the wheelbarrow. It is the one wheeled vehicle of which I am perfect master.