Assignment 3: Three problems of classical cryptanalysis

Deadline: November 22, 23:59
Points: 10 points basic award (problems 1 and 2), 7-point bonus for solutions to problem 3.
Submissions: Please post your submissions as ZIP files where files for each problem are in a separate subdirectory. The programs shall be either in Java or C or C++ and must be reasonably well commented and documented.

Problem 1 – 4 points to be awarded – Mono-alphabetical substitution

Introduction: One historical cryptography method is the mono-alphabetical substitution that substitutes each letter of the alphabet with a different one.

e.g.

Plaintext	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cryptext	Q	W	E	R	T	Y	U	I	O	P	L	K	J	H	G	F	D	S	A	Z	X	C	V	B	N	M

e.g.
The message MY NAME IS BOB will become **JN HQJT OA WGW**

Write a (documented!) program that is able to decrypt the input (ciphertext message) without knowledge of the key. It should read a mono-alphabetic ciphertext from a file and write the corresponding plaintext(s) to a file. Consider only capital letters, and use any dictionary (of words) you see fit to this purpose (indicate the source of this dictionary in the program documentation).

Problem 2 – 6 points to be awarded – A partial bi-gram substitution cipher

In this case:

- The 27 letters of the alphabet (26+_) are substituted with a letter;
- Four pairs of letters and five triples are substituted each one with a special different symbol.

e.g.

Plain	Crypto
ZI	1
ZO	2
CE	3
GI	4
OZZ	5
EZZ	6
CCI	7
GGI	8
SCI	9
A	Q
B	W
C	E
D	R
E	T
F	Y

G	U
H	I
I	O
J	P
K	L
L	K
M	J
N	H
O	G
P	_
Q	D
R	S
S	A
T	Z
U	X
V	C
W	V
X	B
Y	N
Z	M
_	F

Write a (documented!) program that is able to decrypt message without knowing the key. It should read a mono-alphabetic ciphertext from a file and write the corresponding plaintext(s) to a file. Consider only capital letters, and use any dictionary (of words) you see fit to this purpose (indicate the source of this dictionary in the program documentation).

Problem 3 – BONUS – 7 points to be awarded

In this case each group of three letters is substituted with another group of letters, they could be 1, 2, 3 or 4. It is allowed to substitute two different trigrams with the same N-gram.

e.g.
THE➔ABC
ELP➔ABC

PLAIN	CRYPTO
THE	ABC
ELP	ABC
HEL	LKI
ING	HJU
AGE	HTR
CRY	DEW
ITH	QVG
PAG	OKY
RYP	FRT
THI	SDR
YOU	CVG
YPT	VGHI

ALL	ADFS
ART	A
LIN	AB
RTI	PL
STA	K
TAR	KIY
TIN	KIYR
…	…
WIT	
CAN	PTY
ENU	JUY
HIN	LQY
INE	JT
MEN	M
NLI	P

Write a (documented!) program that is able to decrypt message without knowing the key. It should read a mono-alphabetic ciphertext from a file and write the corresponding plaintext(s) to a file. Consider only capital letters, and use any dictionary (of words) you see fit to this purpose (indicate the source of this dictionary in the program documentation).

Bibliography:

Elementary cryptanalysis : a mathematical approach by Abraham Sinkov

Basic Cryptanalysis: HTTP://WWW.UMICH.EDU/~UMICH/FM-34-40-2/

Lecture notes in Cryptanalysis: Dr. Alex Biryukov
http://www.wisdom.weizmann.ac.il/~albi/cryptanalysis/lectures.htm

http://www.gtoal.com/wordgames/cryptograms.html

Software:

http://secretcodebreaker.com/download.html
HTTP://WWW.ICS.UCI.EDU/~EPPSTEIN/SOFTWARE.HTML
www.cryptool.com