Exam #2

Name: Date: Friday, October 14, 2016

Directions: You have a total of 50 minutes for this examination.

- Make sure to put your name on your exam!
- There are a total of 10 questions (worth 10 points each).
- Please write clearly and justify your answers.
- No calculators.
- No materials other than a pen, pencil, and eraser.
- Do not begin until designated.
- Stop working and close exam when time is called.
- Please note that questions are not necessarily in order of difficulty.

Vigenère Cipher

The Vigenère cipher uses an alphabetic key that forms an index to an array of Caesar type ciphers. You can see how this works by looking at the following example that enciphers the word CAT using the key BED. You will see that the key (BED) causes us to first use alphabet 1, then 4 and finally 3.

	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
1	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	A

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

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

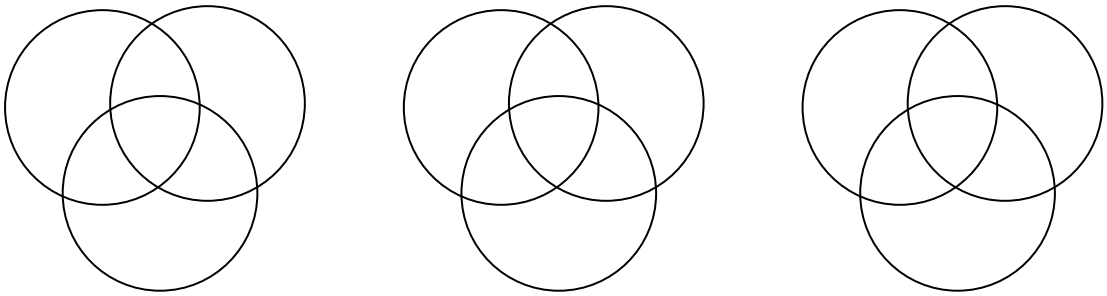
CAT is thus enciphered as DEW. Cracking this code depends on the frequency of common words; repeated strings in the enciphered text will hint at the key length (or a multiple of it) and common words, prefixes or suffixes. Short keys should be easier to crack due to more frequent repetition.

Vigenère Square

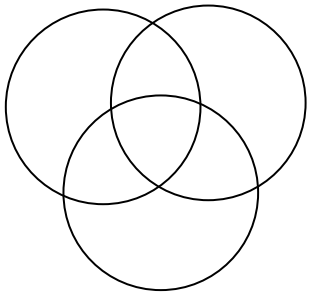
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	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
26	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

 http://www.andrew-scott.co.uk/

Question 1 (10 points): Consider the graph below.
(3 points each)
Use the Circle Diagram Method to find code words for 0101, 0100, and 1011.



(1 point) You receive the message 1111011. Is there a problem?



Question 2 (10 points):

(1 point) What is the distance between 00100 and 01010?

(1 point) What is the distance between 00100 and 01110?

(1 point) What is the distance between 00100 and 00110?

(1 point) What is the distance between 00100 and 00111?

(1 point) What is the distance between 00100 and 11011?

(5 points) Use Nearest-Neighbor Decoding to decode the word 00100 if the code words are 01010, 01110, 00110, 00111, and 11011.

Question 3 (10 points):
Find the Huffman tree representing the following symbols and probabilities.

K 0.03
L 0.20
M 0.07
N 0.31
O 0.34
P 0.05

Question 4 (10 points): Answer the following using modular arithmetic.

a.) (2 points) Pretend that today (Friday, October 14, 2016) is your birthday. What day of the week will your birthday be next year (October 14, 2017)?

b.) (2 points) What day of the week will it be in 100 days?

c.) (2 points) What day of the week was it 49 days ago?

d.) (4 points) Evaluate each of the following.

$45 \pmod{12} =$

$5 \pmod{17} =$

$30 \pmod{7} =$

$18 \pmod{6} =$

Question 5 (10 points):
(4 points) Use the Caesar cipher with (encryption) key 4 to encrypt:

O S K E E W O W W O W

(4 points) Use the decimation cipher with (encryption) key 3 to encrypt:

I L L I N I

(2 points) What is the decryption key for each of these?
The table below may be useful.

Encryption	Decryption
3	9
5	21
7	15
9	3
11	19
15	7
17	23
19	11
21	5
23	17
25	25

Question 6 (10 points): Decrypt the following message.
Caesar Cipher. Cryptography, according to the Roman historian Suetonius, began with Julius Caesar, who "if he had anything confidential to say, he wrote it in cipher, that is, by so changing the order of the letters of the alphabet, that not a word could be made out. If anyone wishes to decipher these, and get at their meaning, he must substitute the fourth letter of the alphabet, namely D, for A, and so with the others."

The encryption key was 19; thus, the decryption key is 7 = -19 (mod 26).

MAX YTNEM WXTK UKNMNL EBXL GHM BG HNK LMTKL UNM BG HNKLXEOXL

Question 7 (10 points): Use the Vigenère cipher with keyword `CAT` to encrypt:

O N E F I S H T W O F I S H

Question 8 (10 points):
(2 points)
Focusing only on candidates A and B, which is the winner using majority rule?

	Voter 1	Voter 2	Voter 3
1st	A	B	B
2nd	B	C	A
3rd	C	A	C

(2 points)
Who is the winner using Condorcet's method?

	Voter 1	Voter 2	Voter 3
1st	A	B	B
2nd	B	C	A
3rd	C	A	C

(6 points) Consider the following preference lists.

	Voter 1	Voter 2	Voter 3	Voter 4	Voter 5	Voter 6	Voter 7
1st	A	A	E	E	A	D	C
2nd	E	E	B	B	C	E	E
3rd	D	D	D	D	D	C	A
4th	C	C	A	A	E	A	D
5th	B	B	C	C	B	B	B

Calculate the winner using:

1. plurality voting,
2. the Borda count,
3. and the Hare system.

Question 9 (10 points): Consider the following preference lists.

	Voter 1	Voter 2	Voter 3	Voter 4	Voter 5	Voter 6
1st	D	B	D	E	D	E
2nd	B	A	B	C	B	C
3rd	A	D	A	A	A	A
4th	C	C	C	B	C	B
5th	E	E	E	D	E	D

(2 points) Calculate the winner using the Borda count.

(2 points) What is the outcome using the Borda count if only Voters 3-6 voted?

(1 points) Why do we usually assume that the number of voters is odd for Borda counts?

(5 points) As Voter 1, can you manipulate the election so Candidate D wins using a Borda count?

	Voter 1	Voter 2	Voter 3	Voter 4	Voter 5	Voter 6
1st		B	D	E	D	E
2nd		A	B	C	B	C
3rd		D	A	A	A	A
4th		C	C	B	C	B
5th		E	E	D	E	D

Question 10 (10 points):
(2 points) Name a voting system in which we have a situation where Candidate A beats B, Candidate B beats C, and Candidate C beats A?

(8 points) Consider these three dice six sided dice.

$$A : 6, 6, 2, 2, 2, 2$$

$$B : 4, 4, 4, 4, 0, 0$$

$$C : 5, 5, 5, 1, 1, 1$$

For a specific dice roll, we say die A beats die B if the value rolled on A is higher than the value rolled on B. We say die A wins over die B if A usually beats B (over 50% of the time). Which of the dice above wins over another?

This page was intentionally left blank for use as scratch paper!
For credit, please clearly indicate the problem number.