Spring 2025 **Math F113X**

Exam 3

Name: Solutions

Section: ☐ **10:30 am (Leah Berman)**
☐ **2:15pm (Jill Faudree)**

Rules:

- Partial credit will be awarded, but you must show your work.
- You may have 1/2 of a standard page of paper ($8.5'' \times 5.5''$) of notes, both sides.
- Calculators are allowed.
- Turn off anything that might go beep during the exam.
- Informational sheets (tabula recta, formulas) are included on the last page of the exam. You may tear them off if you need to.

Problem	Possible	Score
1	12	
2	16	
3	10	
4	16	
5	5	
6	6	
7	20	
8	10	
9	5	
Extra Credit	(5)	
Total	100	

1. (12 points)

a. Encrypt the message EAGLE using an alphabetic Caesar cipher with shift 8 (mapping A to I).

E	A	G	L	E
M	I	O	T	M

← encrypted text

b. Decrypt the message AYCQL if it was encrypted using an alphabetic Caesar cipher with shift 8 (mapping A to I).

A	Y	C	Q	L
S	Q	U	I	D

← decrypted text

2. (16 points)

a. Encrypt the message SPRING IS HERE using a tabular transposition cipher with the encryption keyword JUMBO.

J	U	M	B	O
S	P	R	I	N
G	I	S	H	E
R	E	A	B	C

B	J	M	O	U
I	S	R	N	P
H	G	S	E	I
B	R	A	C	E

answer:
IHB SGR RSA NEC PIE

need columns to be 4 letters tall!

b. Decrypt the message NSEZM ENROM ZSBAB BOADA if it was encrypted using a tabular transposition cipher with the encryption keyword JUMBO.

B	J	M	O	U
N	M	O	B	O
S	E	M	A	A
E	N	Z	B	D
Z	R	S	B	A

J	U	M	B	O
M	O	O	N	B
E	A	M	S	A
N	D	Z	E	B
R	A	S	Z	B

answer:
MOON BEAMS
AND
ZEBRAS

(ZB are extra...)

3. (10 points)

Pick **ONE** of the following. Make sure to clearly identify which one you want graded by checking the appropriate box.

Briefly explain the technique you used to decrypt the message.

a. (Grade this one: ☐) Decrypt the message VFBLV if it was encrypted using a **shifting Caesar cipher** that started with a shift of 4 (mapping A to E).

V	F	B	L	V
R	A	V	E	N

← answer

b. (Grade this one: ☐) Decrypt the message MECZD if it was encrypted using a **Vigenère cipher** with keyword FACE.

F	A	C	E	F
M	E	C	Z	D
H	E	A	V	Y

← answer

4. (16 points)

a. Which of the encryption methods below are vulnerable to being decrypted using frequency analysis? Check the box to indicate it is vulnerable.

☑ Caesar cipher ☐ tabular transposition ☐ Vigenère

☐ shifting Caesar cipher ☐ double transpositon

b. Below is a table defining a **randomly assigned** substitution mapping. Describe one advantage of this encryption mechanism and one disadvantage.

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

Advantage: Hard to crack. Unlike a Caesar shift, knowing one letter isn't enough to know the whole key.

Disadvantage: If you lose the key, it's impossible to easily recreate it!
Also, it's still vulnerable to frequency analysis.

5. (5 points)

You want to encrypt the message YOUR COVER IS BLOWN. LEAVE SAFE HOUSE NOW. using a Vigenère cipher. Pick a code word and explain why it is a good choice. Note: You are **not** asked to encrypt the message!

Because the message is long, I would like to use a long key and preferably something easy to remember such as:

BEYONCELEMONADE

or

MUCHADOABOUTNOTHING

6. (5 points)

Your bill at a restaurant is $38.67 and you want to leave an 18% tip. How much would you add to your bill? Show your calculation.

$(38.67)(0.18) = \$6.96$

7. (20 points)

For each scenario below, identify the formula you should use and then plug into that formula. You do **not** need to calculate the the value.

a. You loan your friend \$400. They agree to pay an annual interest rate of 5% simple interest. Eighteen months later, they repay the loan. How much did they pay you?

$$A = P(1+rt) = 400(1+(0.05)(1.5))$$

b. You deposit \$1000 in an account that earns an annual interest rate of 4.8% APR. The interest is compounding weekly. How much will the account be worth in 10 years?

$$A = P\left(1+\frac{r}{n}\right)^{(nt)} = 1000\left(1+\frac{0.048}{52}\right)^{10\cdot 52}$$

c. You want to take out a loan to buy a \$150,000 home. The bank offers a 30-year mortgage with an interest rate of 6.2%. What will the monthly payments be? (Suppose the interest is compounded monthly.)

$$d = \frac{(150{,}000)\left(\frac{0.062}{12}\right)}{\left(1-\left(1+\frac{0.062}{12}\right)\right)^{12\cdot 30}}$$

d. You deposit \$4000 in an account the earns 2.75% APR compounded daily for 7 years. How much interest did you earn?

$$I = 4000\left(1+\frac{0.0275}{365}\right)^{7\cdot 365} - 400$$

using $A = P + I$ or $I = A - P$

8. (6 points)

It is a fact that

$$441{,}488 = 10{,}000\left(1 + \frac{0.05}{12}\right)^{(12)\cdot(42)}.$$

Suppose this calculation is used to model a savings account. Explain what this calculation indicates about the account parameters.

a. How much was invested at the start? $10,000

b. What was the annual interest rate? 5%

c. How frequently is the interest being compounded? monthly

d. How long was the money invested? 42 years.

e. Explain, in your own words, what the number 441,488 represents.

After 42 years, the savings account has $441,488.

9. (10 points)

Suppose you charge $2000 on a credit card with an annual percentage rate of 29% compounded monthly and you plan to make monthly payments of $40.

a. How much do you owe at the end of the first month? (Show your computation, and actually compute it.)

$$\text{I owe} = 2000\left(1 + \frac{0.29}{12}\right) - 40 = \$2008.33$$

b. What does the calculation in part (a) indicate about when you will pay off the loan?

You will never pay off the loan because you are paying back less than the accumulated interest.

Extra Credit (5 points)

Pick **one** of the two options. Indicate which one you want graded.

(a) (Grade this one: ☐)

Suppose you have the following part of a spreadsheet, where ### represents numbers that have been entered in (but that could be changed).

	A	B	C	D	E
1	P	r	n	t	A
2	###	###	1	1	
3				2	
4				3	
⋮				⋮	

i. Write a formula, using cell references (`A1`, `B2`, `C3`, etc.), to put into cell `E2` to compute the total amount of money at the end of the first year.

$A = P\left(1+\frac{r}{n}\right)^{nt}$ = A2 * (1 + B2)

ii. You want to drag cell `E3` down to automatically compute compound interest (annually compounded) for subsequent years. How would you change your previous formula to be able to do that?

$A = \$A\$2 * \left(1 + \$B\$2\right)^{D2}$

(b) (Grade this one: ☐)

Decrypt the text

S2L53 CDIR8 TEOE4 R3H ← 18 letters. $\frac{18}{4} = 4+\frac{2}{4}$ $\frac{18}{5} = 3+\frac{3}{5}$

if it was encrypted using a double transposition cipher with first keyword JUMBO and second keyword KEYS.

middle word: C S 4, T D 2 R, E 1 L 3, O R 5, H E 8 3

E	K	S	Y
S	C	T	4
2	D	E	R
L	1	O	3
5	R	E	H
3	8		

K	E	Y	S
C	S	4	T
D	2	R	E
1	L	3	O
R	5	H	E
8	3		

B	J	M	O	U
C	T	E	O	H
S	D	1	R	E
4	2	L	5	8
	R	3		3

J	U	M	B	O
T	H	E	C	O
D	E	1	S	R
2	8	L	4	S
R	3	3		

ANSWER
The code is
R 28
L 45
R 33

Formulas

$$A = P + I \qquad A = P(1 + rt) \qquad A = P\left(1 + \frac{r}{n}\right)^{(nt)} \qquad P = \frac{A}{\left(1 + \frac{r}{n}\right)^{(nt)}}$$

$$d = \frac{P\left(\frac{r}{n}\right)}{\left(1 - \left(1 + \frac{r}{n}\right)^{(-nt)}\right)}$$

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