Spring 2026 **Math F113X**

Exam 3

Name: Solutions **Instructor:** _____

Rules:

- Partial credit will be awarded, but you must show your work.
- You may have a 3in $\times$ 5in notecard with writing on both sides.
- Calculators are allowed.
- Turn off anything that might go beep during the exam.

Good luck!

Problem	Possible	Score
1	20	
2	8	
3	18	
4	8	
5	8	
6	14	
7	~~12~~ 16	
8	6	
9	6	
Extra Credit	(4)	
Total	~~100~~ 104	

1. (20 pts)

   (a) (6 pts) **Decrypt** the message NSIZHJ using a **Caesar cipher** with shift 5 (mapping A to F).

N	S	I	Z	H	J
I	N	D	U	C	E

ans: INDUCE

   (b) (6 pts) **Encrypt** the message ROCKET using a **progressive Caesar cipher / sequential shift cipher** starting with a shift of 4 (mapping A to E).

E	F	G	H	I	J	← mapping
R	O	C	K	E	T	
V	T	I	R	M	C	← ciphertext

ans: VTIRM C

   (c) (8 pts) **Decrypt** the message XAPHZNCJ using a **Vigenère cipher** using the keyword FACED.

F	A	C	E	D	F	A	C	← mapping
X	A	P	H	Z	N	C	J	
S	A	N	D	W	I	C	H	← plain text

ans: SANDWICH

2. (8 pts.) **Encrypt** the message I LIKE TO RIDE MY BIKE using a **tabular transposition cipher** with no keyword and rows of length 6. Use extra padding if needed.

1	2	3	4	5	6
I	L	I	K	E	T
O	R	J	D	E	M
Y	B	I	K	E	

=

ans:

IOY LRB III KDK EEE TM

or

IOYLR BIIIK DKEEE TM

3. (18 pts. total)

(a) (8 pts.) Encrypt the plaintext MEET AT LIBRARY using a double transposition cipher and no extra padding. The first keyword is TRIM and the second keyword is TAR

13 letters.

Ciphertext: LITAA RRBET EMY

(b) (10 pts total) A message was encrypted using double transposition with the same keywords in the same order as in part (a): keyword 1 was TRIM, keyword 2 was TAR.

The first step of **decryption** was completed to give MWEOOCN. Answer the following about the **SECOND STAGE** of the decryption of this message.

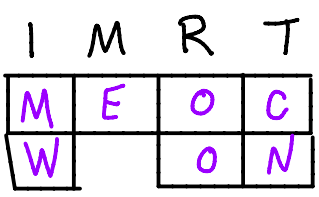
i. (2 pts.) What keyword should be used? TRIM

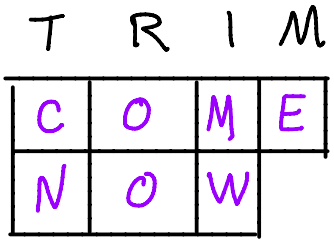
ii. (2 pts.) How many rows (other than the one for the keyword) will be in your table? How many entries in the last row of that table will be left blank?

Number of rows 2

Number of blank entries in last row 1

iii. (6 pts.) Finish the decryption to recover the plaintext.





Plaintext: COME NOW

4. (8 pts.) Give brief answers to the following.

   (a) (2 pts) If a short message (say, 6-8 letters) must be sent securely, is a transposition cipher a good idea? Explain why or why not.

No. It is vulnerable to brute-force unscrambling.

   (b) (2 pts) A long encrypted message is found to have E and T as its most frequent letters. Assuming the plaintext was in English, does this give a clue as to which encryption method might have been used? Explain.

Yes. It suggests that a transposition cipher was used, not a substitution cipher. This is because the common letters (E and T) are still present.

   (c) (2 pts) Why is TABLES a better choice of keyword for a transposition cipher than ACCESS?

ACCESS has double letters making the reordering ambiguous. Even worse, the letters of ACCESS are in alphabetical order. Neither of these issues are found in TABLES.

   (d) (2 pts) Why is BARK a better keyword for a **Vigenère cipher** than NOON?

The point of a Vigenere cipher is to have many different substitutions for a single letter. The word NOON only has two different letters. So each plaintext letter only has <u>two</u> different cipher text replacements. Using BARK, there would be four.

5. (2 pts each for 8 pts total) For each of the following encryption methods, list at least one advantage and at least one disadvantage of the encryption system.

   (a) Caesar cipher

   - Advantage:

- It's simple to encrypt and decrypt.

   - Disadvantage:

- It's vulnerable to guessing, brute forces and frequency analysis.

   (b) Transposition with keyword

   - Advantage:

- No Tabula Recta needed

   - Disadvantage:

- It's vulnerable to unscrambling (esp. short messages)
- A small mistake in transcription can result in a scrambled message.

6. (14 pts) Imagine that at the start of a certain month, you make an opening deposit of $1500 into a savings and account and then you will leave the account alone. Every month after the opening deposit, the amount in the account will grow to be 102% of the previous month's balance.

   For each question below, **write out the calculation you are entering into the calculator in addition to the calculated value.**

   (a) (3pts) What is the amount in the account after 1 month?

   $(1500)(1.02) = \$1530$

   (b) (3 pts) What is the amount in the account after 2 years? (Round to the nearest penny.)

   $(1500)(1.02)^{(2\cdot 12)} = \$2412.66$

   (c) (4 pts) After 4 years, the balance is $2418.35. How much of the balance is **interest**?

   $(2418.35)-(1500) = \$918.35$

   (d) (4 pts) After 5 years, the account has $2725.04. By what percentage has the account grown since the original $1500 deposit?

   $(2725.04)-(1500) = 1225.04$

   $\frac{1225.04}{1500} = 0.81669\ldots = 81.7\%$

7. (4 pts each for 16 pts total) For each scenario, **write out the appropriate formula with numbers substituted in,** but do **not** simplify or compute a final value. No computation is necessary.

   (a) You invest \$4000 into an account that has an interest rate of 2.7% compounded quarterly. Determine the account balance after 10 years.

$$A = 4000\left(1 + \frac{0.027}{4}\right)^{(4)(10)}$$

Using $A = P\left(1 + \frac{r}{n}\right)^{n \cdot t}$

   (b) You plan to take out a 15-year mortgage at 5.4% annual interest compounded monthly, with a maximum monthly payment of \$800. Determine the largest loan amount you could take out.

$$P = \frac{800\left(1 - \left(1 + \frac{0.054}{12}\right)^{-15 \cdot 12}\right)}{\frac{0.054}{12}}$$

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

   (c) An investment earns 8% interest compounded yearly provided you keep your money invested for 20 years. Determine how large the principal would need to be in order to have \$50,000 at the end of the 20 years.

$$P = \frac{50000}{\left(1 + \frac{0.08}{1}\right)^{20 \cdot 1}}$$

Using $P = \frac{A}{\left(1 + \frac{r}{n}\right)^{tn}}$

   (d) TJ loaned a friend \$200. The friend agreed to pay an annual interest rate of 4%, **simple** interest. Six months later the friend repaid the loan. Determine how much the friend paid TJ.

$$A = 200\left(1 + (0.04)\left(\tfrac{1}{2}\right)\right)$$

Using $A = P(1 + rt)$

8. (3 pts each for 6 pts total) You want to buy a $20,000 car. The company is offering an interest rate of 3% APR compounded monthly for 4 years. The monthly payment works out to $443. (You do not need to verify this – take it as given.)

   (a) How much total money will be paid to the loan company? Write out the calculation you are entering into the calculator in addition to the calculated value.

   $(\$443)(12)(4) = \$21,264$

   (b) How much of the total money paid to the loan company is interest?

   $21264 - 20000 = \$1264$

9. (6 pts) You are choosing between two savings accounts with the same annual interest rate, one of which earns **simple** interest and another earns **compound** interest. Which one will have a larger balance in 5 years? Justify your reasoning.

   (a) (2 pts) Which one is larger?

   The one with compound interest.

   (b) (4 pts) Justification:

   Compound interest earns interest on the interest, not just the principal.

Extra Credit (4 pts) You have intercepted the encrypted message below:

BCDFG NPQFZ LSCQJ PTJ

You know the plaintext was in English, and the encryption method was either some kind of substitution cipher or some kind of transposition cipher. Which must it be, and how can you tell from the ciphertext alone?

method: Substitution

how you know: It can't be a transposition cipher because there are no vowels.

FYI
Plaintext is VOWELS ARE IMPORTANT

Formulas

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

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

		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
		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**
0	**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
1	**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
2	**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
3	**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
4	**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
5	**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
6	**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
7	**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
8	**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
9	**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
10	**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
11	**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
12	**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
13	**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
14	**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
15	**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
16	**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
17	**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
18	**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
19	**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
20	**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
21	**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
22	**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
23	**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
24	**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
25	**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