MATH 173A, SAMPLE MIDTERM

17 July 2023

Name: ________________________________

Student ID: ______________________________

Instructions: This 60 minute midterm will be closed book, closed note, and proctored using Zoom proctoring (your webcam must be enabled). No checking cell phones during the exam. Do not type on the computer unless it is to ask the instructor a question through the Zoom chat. Your answers will be graded based on clarity as well as correctness; a correct answer will not receive full credit if the reasoning is difficult to follow. Good luck.

Question	Score	Maximum
0		1
1		
Total		40

	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	❊	ł	ɩ	𓏊	ⵣ	ǀ	є	ɡ	ɷ	𓌻	✻	ɕ	ᛯ ᛯ	ᛯ	ʓ	④	✹	❅	▯	I	✄	b	𓏵	ʝ	ɯ	③
b	☞	➡	L	▼	❤	ʢ	ɐ	⚹	𓃒	✲	ɮ	▭	✥	✭	➢	J	✳	E	j	𓆥	❷	✓	ᛯ	◖	T	𓀠
c	𓋾	△	❷	➘	𓂘	❆	𓉐	ʎ	ƀ	ɤ	③	g	K	𓈗	‖	✤	𓆓	𓍱	ɕ	ᛯ	ɮ	ł	☽	ʈ	ˌ	ƛ
d	➩	▾	𓎛	ₒ	➼	✂	𓂐	ʲ	ᴇ	X ᛉ ᛣ	⬯	g	𓆸	ƀ	ʨ	⊕	➜	➓	→	|	⫯	⚹	𓌉	✪	⑥	𓃝
e	✣	𓅃	⇛	⫲	✦	⌠	✢	𓊛	➎	❀	𓆭	❂	✶	ᛉ	ʞ	ɔ	✙	➍	ɛ	➼	✆	ᴊ	𓉗	❄	☨	β
f	✿	①	ʡ	B	𓅪	➊	↕	ᛯ	ʁ	□	✁	⇨	↯	❏	ь	▲	☹	f	ɟ	☆	✾	M	ɓ	⑦	ɢ	P
g	ᛯ	✬	✂	ᛯ	∅	¦	ᛯ	ᛯ	∾	ɜ	✂	ᛯ	𓂝	ɨ	ᛯ	✄	𓊡	m	➪	●	➡	☞	⟶	✯	ɼ	◯
h	ʿ	ᛯ	ɻ	✂	p	ᛯ	ɹ	➶	ᛯ	𓂾	ᛯ	ɴ	ᛯ	†	⑧	♠	✱	❖	✳	ᛯ	ʐ	➍	◆	ɠ	☻	✦
i	𓍢	Q	❃	𓎡	𓄜	𓎂	★	r	N	⑧	⑤	✡	❄	ʅ	i	ᛯ	ˊ	ǂ	ɣ	ɳ	✇	ƕ	G	✯	❏	χ
j	♫	♦	ǥ	ƶ	❥	✈	✷	ʉ	♣	ʤ	♩	✰	✶	ϙ	⌓	✚	♥	❧	R	𓍱	✤	⋇	ɽ	♣	𓅞	ʛ
k	◈	✡	❦	✽	˂	ɖ	✿	✍	ᛯ	❦	☺	𓋉	ᛯ	đ	✧	𓌫	|	ə	❼	ɗ	✢	𓃭	❖	➶	ʧ	⇨
l	𓂋	⊃	𓏌	⬯	ţ	ᛯ	ı ı ı	⚘	➼	✂	ɧ	ᴜ	➦	✺	𓄸	𓌩	ꞵ	✦	𓅓	ᛯ	⑨	↑	✰	∾	❋	✂
m	⑩	➠	ᛯ	e	➓	o	ᛯ	➻	ɉ	𓍿	▮	ɬ	✵	∞	J	☛	𓏊	❈	ʟ	⍿	ʦ	❦	ᛯ	d	➴	λ
n	ʣ	t	〉	❻	f	𓏇	④	ᛯ	◷	❼	ᛯ	ɿ	✝	𓇋	☎	𓅨	𓄓	𓁐	❁	✠	𓂡	ᛯ	❀	𓌖	✇	v
o	☼	✭	❸	ʄ	✉	ʘ	☺	ɥ	➛	𓂻	♥	⑤	⑨	✤	ƹ	ᛯ	❧	s	ƻ	❦	ɲ	≈	k	Y	ᛯ	ʋ
p	✞	▼	⇨	✆	ħ	♠	✾	ʣ	ɕ	✫	𓅞	⋈	ȡ	𓃟	☞	𓁶	⇨	𓁹	‖	✯	ʙ	ᛯ	❸	✚	☎	☜
q	❉	☙	❙	⤫	𓀀	⌜	➝	❀	⌑	q	𓄣	❦	ɥ	✴	◗	❐	ᛯ	➤	ᛯ	⑥	ʄ	⑦	■	ʕ	✰	❊
r	✹	ᛯ	🔔	𓆛	❅	C	❒	⛥	✪	❂	❋	𓍬	✥	ο	𓀁	𓆳	ᛯ	æ	𓋇	ᛯ	➼	ʠ	𓂝	ƫ	⬬	𓂢
s	𓆼	ʏ	ᛯ	➚	ᛯ	𓅟	≠	❊	∽	↓	u	②	ɪ	ᛯ	✶	ʍ	ᴧ	⑊	➊	✳	⊿	✺	ʣ	➳	ᛯ	𓄿
t	✫	ʐ	∾	ᛯ	❋	⇨	ʨ	ᛯ	✥	✷	☆	⧉	❁	ᛯ	☽	þ	c	➔	ɩ	☆	h	❉	〰	l	☛	✝
u	H	➪	ː	✉	❾	ʖ	❆	э	ʊ	ᛯ	𓅝	D	✡	❦	𓊽	✿	𓅨	ᛯ	ş	𓀀	ᛯ	?	❋	Ɉ	ƙ	✆
v	⛑	ᛯ	❦	✂	ᛯ	U	✌	ɑ	𓀁	❈	ᛯ	ɶ	✿	✽	❄	☎	O	♦	⊘	ᛯ	✠	V	✶	𝅗𝅥	❽	❤
w	②	ъ	đ	►	𓁶	𓎼	☎	ɦ	ᛯ	ᛯ	F	ʗ	❀	n	✇	ʔ	ɳ	▲	ʆ	✂	𓆑	ᛯ	❉	𓆙	𓌪	ᛯ
x	❽	ɩ	ƽ	⊙	▫	⎵	◄	𓍿	ʜ	✳	S	ɸ	ɵ	ᛯ	✈	⧉	ᛯ	❺	⑩	➔	⊜	✂	ʀ	⌝	➧	★
y	☛	✮	a	♪	⇨	➢	θ	ᴀ	𓄑	→	A	ω	𓀀	❊	①	ʳ	ᛯ	ω	✱	ɱ		з	➠	𓆰	☛	✈
z	ᛯ	𓍼	▮	✷	❾	✞	✦	❻	↔	ɜ	𓎛	☘	➴	ʌ	➡	𓆭	✧	✉	ɰ	ˈ	❥	✛	𓎼	ᛯ	ɒ	❖

Sample

One point out of 40 on the midterm will be assigned for your pdf upload being organized and easy to read (for example, the question numbers should be clearly indicated and should be in consecutive order 1, 2, ...).

1. A *digraph substitution cipher* is a substitution cipher in which there is a single ciphertext symbol for every pair of plaintext characters. Thus the key for encryption and decryption will consist of $26 \cdot 26 = 676$ distinct entries. An example of such a key is shown on the previous page. To encipher the phrase "enigma", for instance, we break it up into pairs of characters: [en][ig][ma]. To find the ciphertext symbol for [en], we look in the e-th row and the n-th column to find the symbol "⚘". Similarly, [ig] corresponds to "★" and [ma] corresponds to "⑩". Thus, the plaintext "enigma" corresponds to the ciphertext "⚘ ★ ⑩".
   a. Encrypt the word "chris". (First append a random letter to the end so it has an even number of letters.)
   b. How many choices of key are there, assuming the alphabet of 676 characters is fixed?
   c. What would be one major advantage of this cipher over the usual (26 character) substitution cipher?
   d. What would be one major disadvantage of this cipher over the usual (26 character) substitution cipher?
   e. Would it be useful to look for repeated trigrams in the resulting ciphertext? Why or why not? (I can see an argument for both answers, so the justification is more important than which answer you give.)
   f. A variant of this digraph substitution cipher uses all 676 English bigrams as the ciphertext alphabet. For example, [en] could correspond to [XZ] and [ne] could correspond to [GG] (we don't think of the plaintexts [en] and [ne] as being related, they are treated as completely independent plaintext symbols). Do you think this version would be significantly more secure, significantly less secure, or have about the same as the digraph cipher presented here, which uses 676 distinct individual symbols? Explain your answer.

2. In Lab 1, we gave two procedures for decrypting text that had been encrypted using a Vigenère cipher. Describe one of these two procedures as completely as you can (about 4-5 sentences). There is no need to include Python code, unless it helps with your description.

3. Consider the following Diffie-Hellman Key Exchange. What is suspicious about it? Briefly explain.
   - Alice first posts a prime p and a generator g modulo p.
   - Then Bob posts B and a ciphertext message Y.
   - Then Alice posts A and confirms that she has successfully decrypted Y.

4. a. Adapt the collision algorithm we used in class to find a value of x in $\mathbb{Z}/307\mathbb{Z}$ such that

$$x \cdot 15 \equiv 9 \bmod 307.$$

More than enough data is given in the table below. (Show your work.)

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$i \cdot 9 \bmod 307$	0	9	18	27	36	45	54	63	72	81	90	99	108	117	126	135	144	153	162
$i \cdot 15 \bmod 307$	0	15	30	45	60	75	90	105	120	135	150	165	180	195	210	225	240	255	270
$9 - i \cdot 18 \cdot 15 \bmod 307$	9	46	83	120	157	194	231	268	305	35	72	109	146	183	220	257	294	24	61
$15 - i \cdot 18 \cdot 4 \bmod 307$	15	160	305	143	288	126	271	109	254	92	237	75	220	58	203	41	186	24	169

b. What would be the analogue of the *naive algorithm* for finding a value of x in $\mathbb{Z}/307\mathbb{Z}$ such that

$$x \cdot 15 \equiv 9 \bmod 307?$$

c. Neither the collision algorithm nor the naive algorithm would actually be used to find x in $\mathbb{Z}/307\mathbb{Z}$ such that

$$x \cdot 15 \equiv 9 \bmod 307.$$

Here is a much faster method. Use the extended Euclidean algorithm to find 15^{-1} in $\mathbb{Z}/307\mathbb{Z}$. Then use this to find x. Does this match your answer in part a?

5. Short answer.

a. Explain how a public key cryptosystem and a private key cryptosystem can be used together. (For example, we used both a public key cryptosystem and a private key cryptosystem during the Diffie-Hellman key exchange in Lab 2.)

b. Recall that in a “Chosen Plaintext Attack”, Eve is allowed to choose a plaintext message m and then learns the corresponding ciphertext c. Explain why a public key cryptosystem is worthless if it is vulnerable to chosen plaintext attacks.

c. Assume p is a large prime, and assume g_1 has multiplicative order 10 modulo p, and assume g_2 has multiplicative order 1000 modulo p. Imagine we plot $g_1^x \bmod p$ and $g_2^x \bmod p$. How would you expect these plots to compare to each other?

d. If $f(x) = O(g(x))$, do we necessarily have $g(x) = O(f(x))$? Briefly explain your answer, but you don’t need to give a formal proof.