MATH 173A, 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		10
2		8
3		5
4		10
5		6
Total		40

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. (10 points) In Lab 2, we performed a Diffie-Hellman key exchange. Describe that procedure as completely as you can, up to and including the point where Bob learns the shared secret key k. There is no need to include Python code, unless it helps with your description. Be sure to include the following.
   - Give the formula for how Bob computes k.
   - Clearly indicate what elements were posted on Ed Discussion.

   (Sample level of detail: "Alice chooses a prime p and an element g with order $p-1$ modulo p and posts p and g on Ed Discussion." You don't need to give details of how the elements p and g were computed, nor details of how the Vigenère encryption/decryption were done.)

2. (8 points) The message "bananapeel" was encrypted four separate times, using the following methods. For your convenience, the numeric equivalent of each character is given below.

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	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. Shift cipher

   b. Vigenère cipher with key length 4

   c. Substitution cipher

   d. Digraph subsitution cipher (in which we substitute plaintext pairs of letters aa,ab,...,zz with other pairs of letters AA, AB, ..., ZZ; there are $(26^2)!$ different possible keys for this cipher)

   The resulting ciphertexts are shown below. Match each to the encryption method which was used. Briefly explain your reasoning. (Using process of elimination is fine.)

   i. RIUYDIWCUT

   ii. OZTZTZCHHR

   iii. FNNNNNNDMF

   iv. HGTGTGVKKR

3. (5 points) When performing a Diffie-Hellman Key Exchange, we usually choose a prime p and a generator g (primitive root) modulo p. Even if we don't use a generator, we should still try to use an element with large multiplicative order modulo p. What would be the most serious problem if we used a number with small multiplicative order? Briefly explain your answer.

(Continued on the next page.)

4. (10 points) Consider the Collision Algorithm (*Shanks's Babystep-Giantstep Algorithm*) for computing an integer x such that $g^x \equiv h \bmod p$. The algorithm begins by computing an integer $n := \lfloor\sqrt{N}\rfloor + 1$.

   a. What is N in relation to g, h, p? (Do not assume that g is a primitive root.)

   b. What two lists are then defined by the algorithm? (Give a precise definition of the elements in these two lists.)

   c. Prove that if an element appears in both these two lists, then an integer x exists satisfying $g^x \equiv h \bmod p$.

5. (6 points) Briefly answer each of the following.

   a. Eve claims she can decrypt any piece of Vigenère ciphertext, even if the text is as short as 5 letters, and even if the key length is also 5. Why should you be suspicious of this claim? Be as specific as possible in describing what is suspicious about this claim.

   b. In the context of the Elgamal cryptosystem, assume Eve is able to compute $\mathrm{dlog}_g(A)$, but is not able to compute $\mathrm{dlog}_g(B)$, where A and B were posted in public by Alice and Bob, respectively. Would Eve be able to decrypt Bob's secret message? Explain your answer.