

Math 4981 Midterm

Instructor: Jay Daigle

March 9, 2021

1. This test is due Tuesday at midnight. Logistically, this will work just like the homework: download it, write up your answers, and upload them to Blackboard for me to grade.
2. You will have three hours for this test, though I don't expect you to need all of them. Please write down your start and end times on the test and include that in your upload. You may not spend more than three hours on the test unless you have a specific accommodation.
3. You may consult the course notes during this test, or any notes you have made for yourself.
4. If you have questions, I will be online and responsive during the usual class times. If you want to take the test at a time you know I'll be able to answer any questions quickly, I encourage you to use one of those time slots.
5. You may use a four-function calculator, but nothing more sophisticated. (You can use something like google or wolfram alpha, but only to do basic arithmetic!) Show all your work and explain all calculations you do.
6. Each problem is worth 10 points. The maximum score for this test is 100 points.

Name:

Time Started:

Time Completed:

Problem 1. Alice sends Bob the ciphertext JXU OQH UED JEK I. You suspect Alice is using a Caesar cipher. What is the plaintext?

Problem 2. Here is the key for a monoalphabetic substitution cipher:

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

Encrypt the plaintext `elliptic curve` with this key.

Problem 3. Decrypt the Vigenère ciphertext ARI ZTE VEM VAR X with the keyword `enigma`.

Problem 4. Encrypt the plaintext `abelian group` with an autokey cipher, using the key word `ring`.

Problem 5. Decrypt the ciphertext KGMZJU if it is encrypted by a Hill cipher with encryption key $K = \begin{bmatrix} 3 & 5 \\ 7 & 12 \end{bmatrix}$.

Problem 6. Suppose 50% of the messages you get are spam. You install a spam filter that removes 99% of spam messages and only 5% of non-spam messages. What is the probability that a rejected message was wrongly classified and actually not spam?

Problem 7. Suppose a cryptosystem has five messages, with the probability distribution $P(m_1) = 1/2, P(m_2) = 1/4, P(m_3) = 1/8, P(m_4) = P(m_5) = 1/16$. What is $H(M)$? Construct a cryptosystem using these messages and five keys that has perfect secrecy.

Problem 8. Alice and Bob want to generate a shared secret with a Diffie-Hellman scheme. They choose the prime $p = 29$ and generator $g = 2$. Alice chooses $a = 5$ and receives $B = 10$ from Bob. What does Alice transmit to Bob, and what is the shared secret?

Problem 9. Alice and Bob are using an ElGamal encryption scheme, now using the prime $p = 59$ and generator $g = 2$. Alice chooses the private key $a = 7$. What is her public key?

If Bob sends her the ciphertext $(8, 20)$, what is the plaintext message he's trying to send?

Problem 10. Alice and Bob have now moved on to using RSA encryption. Bob publishes a public key of $(143, 7)$. If Alice wants to send the message $m = 5$, what should she transmit?