Math 4981 Midterm Solutions

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?

Solution: `the yar eon tou s` or "They are on to us".

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.

Solution:

`XIIDEZDM MKJNX`

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

Solution: `wea the rre por t` or "weather report".

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

Solution:

`RJR RIB RRZ OHV`

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

Solution:

The text `KGMZJU` becomes the numbers `10 6 12 25 9 20`. We see that $\det K = 26 - 35 = 1$ so $K^{-1} = \begin{bmatrix} 12 & -5 \\ -7 & 3 \end{bmatrix}$. Then we have

$$\begin{bmatrix} 12 & -5 \\ -7 & 3 \end{bmatrix} \begin{bmatrix} 10 \\ 6 \end{bmatrix} = \begin{bmatrix} 90 \\ -52 \end{bmatrix} \equiv \begin{bmatrix} 12 \\ 0 \end{bmatrix}$$
$$\begin{bmatrix} 12 & -5 \\ -7 & 3 \end{bmatrix} \begin{bmatrix} 12 \\ -1 \end{bmatrix} = \begin{bmatrix} 149 \\ -87 \end{bmatrix} \equiv \begin{bmatrix} 19 \\ 17 \end{bmatrix}$$
$$\begin{bmatrix} 12 & -5 \\ -7 & 3 \end{bmatrix} \begin{bmatrix} 9 \\ -6 \end{bmatrix} = \begin{bmatrix} 138 \\ -81 \end{bmatrix} \equiv \begin{bmatrix} 8 \\ 23 \end{bmatrix}$$

Thus the plaintext is `matrix`.

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?

Solution: We have $P(S) = .5$, $P(\text{reject}|S) = .99$, and $P(\text{reject}|\neg S) = .05$. Then

$$P(\neg S|\text{reject}) = \frac{P(\text{reject}|\neg S)P(\neg S)}{P(\text{reject}|\neg S)P(\neg S)(+P(\text{reject}|S)P(S)} = \frac{.05 \cdot .5}{.05 \cdot .5 + .99 \cdot .5} = \frac{5}{104} \approx .048.$$

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.

Solution:

$$H(M) = -\left(\frac{1}{2}\log(1/2) + \frac{1}{4}\log(1/4) + \frac{1}{8}\log(1/8) + \frac{1}{8}\log(1/16)\right) = \frac{1}{2} + \frac{1}{2} + \frac{3}{8} + \frac{1}{2} = \frac{15}{8}.$$

If all keys have equal probability, then the following cryptosystem is perfectly secure:

	m_1	m_2	m_3	m_4	m_5
k_1	c_1	c_2	c_3	c_4	c_5
k_2	c_2	c_3	c_4	c_5	c_1
k_3	c_3	c_4	c_5	c_1	c_2
k_4	c_4	c_5	c_1	c_2	c_3
k_5	c_5	c_1	c_2	c_3	c_4

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?

Solution:

Alice transmits $A = g^a = 2^5 = 32 \equiv 3 \mod 29$.

The shared secret is $B^a = 10^5 = 100^2 \cdot 10 \equiv 13^2 \cdot 10 = 169 \cdot 10 \equiv -5 \cdot 10 \equiv -50 \equiv 8 \mod 29$.

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?

Solution: Alice's public key is $A = 2^7 = 128 \equiv 10 \mod 59$.

Alice computes $x = c_1^a \equiv 8^7 \equiv 64^3 \cdot 8 \equiv 5^3 \cdot 8 \equiv 125 \cdot 8 \equiv 7 \cdot 8 \equiv -3 \mod 59$. We have $x^{-1} = -20$, so then we have $m = x^{-1} \cdot 20 = -400 \equiv 13$.

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?

Solution:

Alice computes $c = m^e = 5^7 \equiv 125^2 \cdot 5 \equiv (-18)^2 \cdot 5 \equiv 324 \cdot 5 \equiv 38 \cdot 5 \equiv 190 \equiv 47 \mod 143$. So Alice transmits $m = 47$.