Math 139 Solution
Final Exam May 2003

---

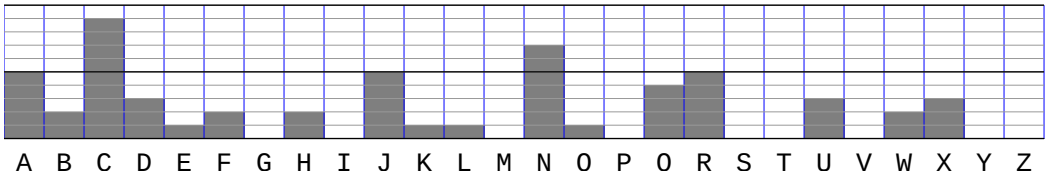
1. Decrypt the following, which has been enchipered using a shift cipher.

   CQNCA XDKUN FRCQC QNAJC AJLNR

   BCQJC NENWR OHXDF RWHXD ANBCR

   UUJAJ C

   Solution: Here's a frequency histogram of the letters in the cryptogram.



   If plaintext `e` goes to ciphertext `C`, then our message contains no `a`'s, which seems unlikely. The better fit has plaintext `e` going to ciphertext `N`. Then plaintext `a` goes to ciphertext `J`.

   Setting the cipherdisk to this shift, we find the decrypted text:

   > The trouble with the rat race is that even if you win
   > you're still a rat.

2. Decrypt the following, given that it was encrypted using an affine cipher, and that the first three letters of the plaintext are `the`.

   NHMZK LWOGM PLMXG OBMLE LLOXA

   RURRJ MIZKL OGYHM KL

Solution: The given crib says that the encryption keys a and b satisfy

$$\begin{aligned} 19a &+ b \equiv 13 \pmod{26} \\ 7a &+ b \equiv 7 \pmod{26} \\ 4a &+ b \equiv 12 \pmod{26} \end{aligned}$$

Subtracting the third of these congruences from the second yields

$$\begin{aligned} 3a &\equiv -5 \pmod{26} \\ &\equiv 21 \pmod{26} \end{aligned}$$

We multiply both sides of this last congruence by 3^{-1} (which is 9, modulo 26) to get

$$\begin{aligned} a &\equiv 9 \times 21 \pmod{26} \\ &\equiv 7 \pmod{26} \end{aligned}$$

Substituting this value back into the congruence $4a + b \equiv 12 \pmod{26}$, we get

$$28 + b \equiv 12 \pmod{26}$$

which implies that $b = 10$. The encryption keys are $a = 7$, $b = 10$.

The encryption function is thus

$$y = 7x + 10 \text{ MOD } 26$$

To find the decryption function, we write

$$x \equiv 7y + 10 \pmod{26}$$

and solve for y, getting

$$\begin{aligned} y &= (15x - 20) \text{ MOD } 26 \\ &= (15x + 6) \text{ MOD } 26 \end{aligned}$$

Using this equation, we can set up a decryption alphabet:

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:	g	v	k	z	o	d	s	h	w	l	a	p	e	t	i	x	m	b	q	f	u	j	y	n	c	r

Finally, we recover the plaintext as

Therapy is expensive; popping bubble wrap is cheap.

3. Decrypt the following, given that it was encrypted using a keyword cipher, the keyword has four letters, and the first two words of the plaintext are `always be`.

   EJVEX QABQG LSBPB VFBRF BPXMT

   KBELG RMPLM R

   Solution: We begin rebuilding the encryption alphabet, using the given crib. We get

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:	E	A			B						J							Q					V		X	

   We can fill in the ciphertext letters between `B` and `J`, those between `J` and `Q`, and the `W`:

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:	E	A			B	C	D	F	G	H	I	J	K	L	M	N	O	P	Q				V	W	X	

   Of the remaining two letters in the keyword, one has to be either `R`, `S`, or `T`, and the other has to be either `Y` or `Z`. We suspect that the keyword is `EASY`.

   To get more data, we could start to decrypt the message. Using the letters we have so far, we get the partial plaintext:

   alway sbesi n?ere whe?h eryo?

   meani ?orno ?

   The cryptogram reads "Always be sincere, whether you mean it or not." Given this, we can complete our alphabet, and discover that the keyword was, indeed, `EASY`.

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

4. The following text was enciphered using a Vigenère cipher with a six-letter keyword. Given that the first word of the plaintext is `never`, find the keyword and decrypt the text.

RWXEG XVMUT PWXGE KQVSC GRLLS

KOAGV MWFTD EXJCV TPEYG NI

Solution: Using our cipherdisk and the given crib, we find that the first five letters of the keyword are E, S, C, A, and P.

We can think of only one six-letter English word beginning with ESCAP, and we guess that the keyword is ESCAPE. The decryption is

> Never trust a stockbroker who's married to a travel agent.

5. Eve's sock drawer is a mess. It contains, all jumbled together, ten white socks, eight black socks, six blue socks, and (for some reason) three red socks.

   Early in the morning, before even opening her eyes, Eve reaches into the drawer and pulls out two socks at random. What is the probability that Eve selects two socks of the same color?

   Solution: Eve is selecting two of the twenty-seven socks in the drawer, so there are $C(27, 2) = 351$ possible outcomes in this experiment.

   She can select a pair of white socks in $C(10, 2) = 45$ ways; a pair of black socks in $C(8, 2) = 28$ ways; a pair of blue socks in $C(6, 2) = 15$ ways; and a pair of red socks in $C(3, 2) = 3$ ways. The total number of ways in which Eve can select a pair of matching socks is

   $$45 + 28 + 15 + 3 = 91.$$

   The probability of her selecting matching socks is $91/351 \approx 26\%$.

6. Agnes and Bart both work for the same major airline, but in offices in different parts of the country. Each needs to know the other's daily price forecasts for a promising new route (Newark to Timmins, Ontario), but these forecast numbers must be kept secret from the other major airlines.

   They meet at a conference in Honolulu, and decide to use prime-modulus cryptography to conceal their price forecasts. They select the numbers $p = 525299$ and $e = 30133$.

   (a) Agnes's office figures that the fare for the new route should be \$319. She encrypts this and surreptitiously includes the ciphertext in her next casual e-mail to Bart. What is Agnes's ciphertext?

   Solution: She computes $319^{30133} \bmod 525299$, which is 181480.

(b) In his reply, Bart causally mentions the number 473185. What is Bart's idea for the fare for the new route?

Solution: First Agnes needs to find $d = 30133^{-1} \pmod{525298}$. She uses her calculator to find $d = 207065$.

Next Agnes calculates

$$473185^{207065} \text{ MOD } 525299 = 276.$$

Bart's office wants to price the new route at \$276.

7. Alma's birthday is coming up. Her e-mail pen-pal, Barb, wants to know the exact date, and how old Alma is. Alma is happy to share this information with Barb, but she would prefer that her neighbor, Evan (who somehow reads all her e-mail and is also kind of creepy), be kept in the dark.

Barb suggests that Alma encrypt her date of birth (in the form YYMMDD) using RSA encryption. Barb selects two primes, $p = 977$ and $q = 1427$, and an encryption exponent $e = 570223$ (which happens to be her own date of birth).

(a) What information does Barb send to Alma (and, unknowingly, to Evan as well)?

Solution: She sends Alma the modulus, 1394179, and the encryption exponent, 570223.

(b) Alma replies that her (encrypted) date of birth is 1293662. When is Alma's next birthday, and how old will she be?

Solution: Barb needs to determine her decryption exponent,

$$\begin{aligned} d &\equiv e^{-1} \pmod{(p-1)(q-1)} \\ &\equiv 570223^{-1} \pmod{1391776} \\ &\equiv -472433 \pmod{1391776} \\ &\equiv 919343 \pmod{1391776} \end{aligned}$$

Next she computes

$$1293662^{919343} \text{ MOD } 1394179 = 610527.$$

Alma was born on May 27, 1961, so she will celebrate her 42^{nd} birthday on May 27.

8. Evan orders some weapons-grade plutonium from wmdsupply.com. In order to arrange for delivery, he needs to send his address to the company's website. For reasons connected with some of his hobbies, he'd prefer to encrypt this information.

   The website wmdsupply.com uses RSA encryption, so Evan sends out a request for wmdsupply's encryption keys. Curiously, he receives two replies:

Hi! This is wmdsupply.com. Here's our certificate: $m = 703751$ $e = 52433$ $\sigma = 396487$	Hi! This is wmdsupply.com. Here's our certificate: $m = 802591$ $e = 87237$ $\sigma = 361360$

   Evan knows that wmdsupply.com has a certificate from his trusted friend CA, whose RSA public keys are $m_{\text{CA}} = 1511381$ and $e_{\text{CA}} = 196303$. He also knows that CA uses a simple hash function, just adding the numbers in any message to get a message digest.

   Which public keys should Evan use to send his address to wmdsupply, and why?

   Solution: The message digest for the first reply is 756184. Evan checks to see if the signature matches this digest. He computes

   $$\begin{aligned} \sigma^{e_{\text{CA}}} \text{ MOD } m_{\text{CA}} &= 396487^{196303} \text{ MOD } 1511381 \\ &= 1723 \end{aligned}$$

   which does not match the message digest. The first reply appears to be forged.

   The message digest for the second reply is 889828. Evan computes

   $$\begin{aligned} \sigma^{e_{\text{CA}}} \text{ MOD } m_{\text{CA}} &= 361360^{196303} \text{ MOD } 1511381 \\ &= 889828. \end{aligned}$$

   Since this does match the message digest, Evan concludes that the second reply was signed by CA.

Sources of the quotes used in the cryptograms:

1. *The trouble with the rat race is that even if you win, you're still a rat.*

   This is most often attributed to Lily Tomlin.

2. *Therapy is expensive; popping bubble wrap is cheap.*

   This appears on scores of websites and on at least one bumper sticker, but I was unable to find a site giving an attribution.

3. *Always be sincere, whether you mean it or not.*

   This may have originated with the lyricist Michael Flanders. It appears in his song "The Reluctant Cannibal" (c1955).

4. *Never trust a stockbroker who's married to a travel agent.*

   This, too, appears on numerous websites, but I could not determine its origin.