Math 139 Solution
Quiz 3 28 February 2003

1. A cryptanalyst working on a monoalphabetic, keyword-enciphered cryptogram uses frequency counts and cribs to construct the following partial *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:	h	i	e		d		l		a		o		q	b	r	s	t				u		v			

Find the keyword. (Hint: it's in the *encryption* alphabet.)

Here's the corresponding partial encryption alphabet.

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:	I	N		E	C			A	B			G			K		M	O	P	Q	T	V				

We suspect that the keyword ends just before the ciphertext A. The letters between B and G must be D and F, since E and C occur in the keyword. Simlarly, we can fill in H, J, and L, and all the letters after V. 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:	I	N		E	C			A	B	D	F	G	H	J	K	L	M	O	P	Q	T	V	W	X	Y	Z

Now we know the letters in the keyword. In addition to I, N, E, and C, there must be an R, an S, and a U. The keyword has the form IN_EC___, with the letters R, S, and U filling in three of the blanks. The word INSECURE fits that pattern.

2. The following Einstein quote was encrypted using a Vigenère cipher with the keyword EINSTEIN. Decrypt it.

XQZWB WEUEB VKBRL VGIGW WFGNG TBUD

Solution: Following the convention in the book, we write the keyword above the text and decrypt letter by letter using a cipher disk. We get

EINST	EINEI	NSTEI	NEINS	TEINE	INST
XQZWB	WEUEB	VKBRL	VGIGW	WFGNG	TBUD
timei	swhat	isind	icate	dbyac	lock

"Time is what is indicated by a clock."