

My signature testifies that I have neither given nor received aid on this quiz.

Name: \_\_\_\_\_

SUID: \_\_\_\_\_

**CIS 400/628**  
**Spring 2005**  
**Quiz 1**

1. (5 pts.) Encrypt the following phrase with a multiplicative cipher and key 3.

Read *Cryptonomicon* by Neal Stephenson!

The first answer is the “normal” convention of  $A = 0$ , the second is the Lewand convention of  $A = 1$ .

a	b	c	d	e	f	g	h	i	j	k	l	m
A	D	G	J	M	P	S	V	Y	B	E	H	K
C	F	I	L	O	R	U	X	A	D	G	J	M

n	o	p	q	r	s	t	u	v	w	x	y	z
N	Q	T	W	Z	C	F	I	L	O	R	U	X
P	S	V	Y	B	E	H	K	N	Q	T	W	Z

r	e	a	d		c	r	y	p	t	o	n	o	m	i	c	o	n
Z	M	A	J		G	Z	U	T	F	Q	N	Q	K	Y	G	Q	N
B	O	C	L		I	B	W	V	H	S	P	S	M	A	I	S	P

b	y		n	e	a	l		s	t	e	p	h	e	n	s	o	n
D	U		N	M	A	H		C	F	M	T	V	M	N	C	Q	N
F	W		P	O	C	J		E	H	O	V	X	O	P	E	S	P

2. (1 pt.) Give the definition of “relatively prime” in terms of gcd.

$$a, b \in \mathbb{Z}^+ \iff \gcd(b, 1) = 1.$$

3. (4 pts.) Consider the set  $S = \{x | x \in \mathbb{Z} \text{ and } x > 1\}$ . Prove that any two consecutive integers in  $S$  are relatively prime.

$x, x + 1$  are relatively prime iff  $\gcd(x + 1, x) = 1$ .

$\gcd(x + 1, x) = \gcd(x, 1)$  by the gcd algorithm ( $x + 1 = 1 \cdot x + 1$ ).

$\gcd(x, 1) = 1$ .