Fall 2006
Chris Christensen
MAT/CSC 483

Multiplicative Ciphers

> *It is evident from the relative ease with which the Caesar Cipher – or its generalization to an arbitrary number of positions of shift – has been solved, that such a system offers very little security. Let us think up a different method of enciphering a message. Instead of adding a key number to the equivalents of the plain text letters, we shall multiply by the key number.* Abraham Sinkov, *Elementary Cryptanalysis.*

Cryptography of Multiplicative Ciphers

Caesar ciphers are encrypted by adding modulo 26 (C = p + key mod 26, where C is ciphertext and p is plaintext) and are decrypted by adding the inverse of the key. It seems reasonable (at least to a mathematician like Sinkov) to consider what would happen if we encrypted by multiplying modulo 26; i.e., C = mp mod 26 where is m is called the multiplicative key. But, things do not go as well as they did for Caesar ciphers. Decryption is not always possible. Let's look at some examples.

Let us see what goes wrong when we try using 2 as a multiplicative key.

a	1	multiplied by 2 modulo 26 is	2	which corresponds to	B
b	2		4		D
c	3		6		F
d	4		8		H
e	5		10		J
f	6		12		L
g	7		14		N
h	8		16		P
i	9		18		R
j	10		20		T
k	11		22		V
l	12		24		X
m	13		26		Z
n	14		2		B
o	15		4		D
p	16		6		F
q	17		8		H
r	18		10		J
s	19		12		L
t	20		14		N
u	21		16		P
v	22		18		R
w	23		20		T
x	24		22		V
y	25		24		X
z	26		26		Z

Notice that not all of the letters of the alphabet appear in the ciphertext alphabet; obviously only letters that correspond to even integers can appear. The ciphertext alphabet consists of two copies of the letters that correspond to the even integers in 1, … 26; we have two copies of the string BDFHJLNPRTVXZ. This scheme could not be used for a cipher because there is no inverse to the process; there is no unique way to go backwards from the ciphertext to the plaintext. For example, ciphertext N could be either plaintext g or t; there is no way to tell which is correct. Even worse, there are 32 possible decryptions of BDJLJ. (Can you guess which is correct?) This is called a polyphonic substitution; more than one plaintext letter may correspond to the same ciphertext letter. Although sometimes polyphonic substitution is used in cryptography, it is generally only used for a few letters. Polyphonic substitutions do not give unique decryptions. If the multiplicative key is 2, each ciphertext letter corresponds to two plaintext letters; this is a two-to-one mapping. Remember, for an inverse to exist – to be able to decrypt – we need a one-to-one mapping.

A similar thing happens with multiplication by 4 modulo 26.

a	1	multiplied by 4 modulo 26 is	4	which corresponds to	D
b	2		8		H
c	3		12		L
d	4		16		P
e	5		20		T
f	6		24		X
g	7		2		B
h	8		6		F
i	9		10		J
j	10		14		N
k	11		18		R
l	12		22		V
m	13		26		Z
n	14		4		D
o	15		8		H
p	16		12		L
q	17		16		P
r	18		20		T
s	19		24		X
t	20		2		B
u	21		6		F
v	22		10		J
w	23		14		N
x	24		18		R
y	25		22		V
z	26		26		Z

Again, notice that not all of the letters of the alphabet appear in the ciphertext alphabet. The ciphertext alphabet consists of two copies of the string DHLPTXBFJNRVZ; this is also a two-to-one mapping. There is no inverse to this process either.

Let us see what happens when 3 is used as a multiplicative key.

a	1	multiplied by 3 modulo 26 is	3	which corresponds to	C
b	2		6		G
c	3		9		I
d	4		12		L
e	5		15		O
f	6		18		R
g	7		21		U
h	8		24		X
i	9		1		A
j	10		4		D
k	11		7		G
l	12		10		J
m	13		13		M
n	14		16		p
o	15		19		S
p	16		22		V
q	17		25		Y
r	18		2		B
s	19		5		E
t	20		8		H
u	21		11		K
v	22		14		N
w	23		17		Q
x	24		20		T
y	25		23		W
z	26		26		Z

This time all of the letters of the alphabet appear exactly once in the ciphertext alphabet; there is an inverse to this process because each ciphertext letter comes from a unique plaintext letter. For example, ciphertext `D` comes from plaintext `j`. This is a one-to-one mapping.

But, notice that (unlike the Caesar cipher) the order of the ciphertext alphabet is scrambled.

Why do some multipliers give a one-to-one mapping and others do not? The answer is that 2 and 26 have a common divisor of 2, and 4 and 26 have a common divisor of 2, but 3 and 26 have no common divisor. Here are two more examples.

First, try a multiplicative key of 6. Because 6 and 26 have a common divisor of 2, we might guess that this should not work as a multiplicative key. We

might suspect that multiplication by 6 mod 26 will result in a two-to-one mapping.

a	1	multiplied by 6 modulo 26 is	6	which corresponds to	F
b	2		12		L
c	3		18		R
d	4		24		X
e	5		4		D
f	6		10		J
g	7		16		P
h	8		22		V
i	9		2		B
j	10		8		H
k	11		14		N
l	12		20		T
m	13		26		Z
n	14		6		F
o	15		12		L
p	16		18		R
q	17		24		X
r	18		4		D
s	19		10		J
t	20		16		P
u	21		22		V
v	22		2		B
w	23		8		H
x	24		14		N
y	25		20		T
z	26		26		Z

And, we are correct. As we expected, not all the letters of the alphabet appear in the ciphertext alphabet; the ciphertext alphabet consists of the string FLRXDJPVBHNTZ repeated twice. This is a two-to-one mapping.

Notice that we did not need to do all of the multiplications. We could have begun with 1 which corresponds to plaintext a and multiplied it by 6 modulo 26 which corresponds to ciphertext F. Then we could have counted 6 more letters to get the next ciphertext letter L, 6 more to get the next ciphertext letter R, etc. After doing this 13 times, we return to F because 13×6 is a multiple of 26. $6 + 13 \times 6 \equiv 6 \bmod 26$. Then the string repeats.

What should happen when we use a multiplicative key of 9?

a	1	multiplied by 9 modulo 26 is	9	which corresponds to	I
b	2		18		R
c	3		1		A
d	4		10		J
e	5		19		S
f	6		2		B
g	7		11		K
h	8		20		T
i	9		3		C
j	10		12		L
k	11		21		U
l	12		4		D
m	13		13		M
n	14		22		V
o	15		5		E
p	16		14		N
q	17		23		W
r	18		6		F
s	19		15		O
t	20		24		X
u	21		7		G
v	22		16		P
w	23		25		Y
x	24		8		H
y	25		17		Q
z	26		26		Z

As expected, all the letters of the alphabet appear in the ciphertext alphabet. This is a one-to-one mapping.

Again, we could have begun with 1 which corresponds to plaintext a and multiplied it by 9 modulo 26 which corresponds to ciphertext I. Then we could have counted 9 more letters to get the next ciphertext letter R, 9 more to get the next ciphertext letter A, etc. We do not come to a multiple of 26 until we do this process 26 times.

The process of encrypting by multiplying by 6 modulo 26 does not have an inverse and would not work as a cipher, but the process of encrypting by multiplying by 9 modulo 26 does have an inverse and would work as a cipher.

To recap, multiplication by 2, 4, or 6 modulo 26 does not work as a cipher because in these cases there is no inverse to the multiplication, but

multiplication by 3 or 9 modulo 26 does work as a cipher because in these cases there is an inverse to the process.

Notice that when the multiplier was 2 or 4 or 6, 2 was the greatest common divisor of our multiplier and 26; the string of ciphertext letters was repeated twice. When the multiplier was 3 or 9, the greatest common divisor of our multiplier and 26 was 1 (we say that 3 and 26 are relatively prime and 9 and 26 are relatively prime); there was no repetition of ciphertext letters.

Let us examine two extreme cases. The worst case would be multiplication by 26 modulo 26 -- every plaintext letter would be mapped to ciphertext `Z`. This is a 26-to1 mapping. If we multiplied by 13 modulo 26, we would get

a	1	multiplied by 13 modulo 26 is	13	which corresponds to	M
b	2		26		Z
c	3		13		M
d	4		26		Z

Etc. The ciphertext alphabet consists of thirteen repetitions of the string `MZ`. This is a thirteen-to-one mapping. Notice that the greatest common divisor of 26 and 26 is 26 and the greatest common divisor of 13 and 26 is 13.

The Number of Possible Keys

The only multipliers that are possible are those that result in one-to-one mappings. By trying all 26 possible multipliers modulo 26, we would discover that only 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, and 25 have inverses. These are the 12 positive integers that are less than 26 and relatively prime to 26. So, there are only 12 possible multiplicative keys, and one of them is 1 which would make the ciphertext alphabet the same as the plaintext alphabet.

Let’s look more carefully at multiplication modulo 26. Here is the multiplication table.

Multiplication modulo 26

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
2	2	4	6	8	10	12	14	16	18	20	22	24	26	2	4	6	8	10	12	14	16	18	20	22	24	26
3	3	6	9	12	15	18	21	24	1	4	7	10	13	16	19	22	25	2	5	8	11	14	17	20	23	26
4	4	8	12	165	20	24	2	6	10	14	18	22	26	4	8	12	16	20	24	2	6	10	14	18	22	26
5	5	10	15	20	25	4	9	14	19	24	3	8	13	18	23	2	7	12	17	22	1	6	11	16	21	26
6	6	12	18	24	4	10	16	22	2	8	14	20	26	6	12	18	24	4	10	16	22	2	8	14	20	26
7	7	14	21	2	9	16	23	4	11	18	25	6	13	20	1	8	15	22	3	10	17	24	5	12	19	26
8	8	16	24	6	14	22	4	12	20	2	10	18	26	8	16	24	6	14	22	4	12	20	2	10	18	26
9	9	18	1	10	19	2	11	20	3	12	21	4	13	22	5	14	23	6	15	24	7	16	25	8	17	26
10	10	20	4	14	24	8	18	2	12	22	6	16	26	10	20	4	14	24	8	18	2	12	22	6	16	26
11	11	22	7	18	3	14	25	10	21	6	17	2	13	24	9	20	5	16	1	12	23	8	19	4	15	26
12	12	24	10	22	8	20	6	18	4	16	2	14	26	12	23	10	22	8	20	6	18	4	16	2	14	26
13	13	26	13	26	13	26	13	26	13	26	13	26	13	26	13	26	13	26	13	26	13	26	13	26	13	26
14	14	2	16	4	18	6	20	8	22	10	24	12	26	14	2	26	4	18	6	20	8	22	10	24	12	26
15	15	4	19	8	23	12	1	16	5	20	9	24	13	2	17	6	21	10	25	14	3	18	7	22	11	26
16	16	6	22	12	2	18	8	24	14	4	20	10	26	16	6	22	12	2	18	8	24	14	4	20	10	26
17	17	8	25	16	7	24	15	6	23	14	5	22	13	4	21	12	3	20	11	2	19	10	1	18	9	26
18	18	10	2	20	12	4	22	14	6	24	16	8	26	18	10	2	20	12	4	22	14	6	24	16	8	26
19	19	12	5	24	17	10	3	22	15	8	1	20	13	6	25	18	11	4	23	16	9	2	21	14	7	26
20	20	14	8	2	22	16	10	4	24	18	12	6	26	20	14	8	2	22	16	10	4	24	18	12	6	26
21	21	16	11	6	1	22	17	12	7	2	23	18	13	8	3	24	19	14	9	4	25	20	15	10	5	26
22	22	18	14	10	6	2	24	20	16	12	8	4	26	22	18	14	10	6	2	24	20	16	12	8	4	26
23	23	20	17	14	11	8	5	2	25	22	19	16	13	10	7	4	1	24	21	18	15	12	9	6	3	26
24	24	22	20	18	16	14	12	10	8	6	4	2	26	24	22	20	18	16	14	12	10	8	6	4	2	26
25	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	26
26	26	26	26	26	26	26	26	26	26	26	26	26	26	26	26	26	26	26	26	26	26	26	26	26	26	26

Notice that only 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, and 25 have multiplicative inverses modulo 26. Here are the possible multipliers and their inverses:

Number	1	3	5	7	9	11	15	17	19	21	23	25
Multiplicative inverse	1	9	21	15	3	19	7	23	11	5	17	25

$1\times 1 = 1 \bmod 26$, $3\times 9 = 26 = 1 \bmod 26$, $5\times 21 = 105 = 1 \bmod 26$, $7\times 15 = 105 = 1 \bmod 26$, $11\times 19 = 209 = 1 \bmod 26$, $17\times 23 = 391 = 1 \bmod 26$, and $25\times 25 = 625 = 1 \bmod 26$. But, 2, for example, does not have an inverse; there is no number mod 26 that 2 can be multiplied by that will result in 1.

Here is an example of a multiplicative cipher with multiplicative key 7.

Multiplicative cipher
Multiplicative key = 7

a	1	7	G
b	2	14	N
c	3	21	U
d	4	2	B
e	5	9	I
f	6	16	P
g	7	23	W
h	8	4	D
i	9	11	K
j	10	18	R
k	11	25	Y
l	12	6	F
m	13	13	M
n	14	20	T
o	15	1	A
p	16	8	H
q	17	15	O
r	18	22	V
s	19	3	C
t	20	10	J
u	21	17	Q
v	22	24	X
w	23	5	E
x	24	12	L
y	25	19	S
z	26	26	Z

The disjoint cycles of the key are

(agweikyscuqo)(bntjrvxlfphd)(m)(z).

All 12 multiplicative cipher keys fix the letters z and m. That z is fixed is easy to see.

Using our plaintext letter-to-number scheme, z corresponds to 26. If k_m is the multiplicative key, then the ciphertext letter corresponding to z is

$$C = k_m \times 26 \bmod 26 = 0 \bmod 26.$$

z (26) corresponds to Z (0 = 26 mod 26); so, z is fixed.

Seeing that m (13) is fixed is only a little harder. Each of the 12 multiplicative keys is odd; therefore, each can be written as $k_m = 2n + 1$, where n is an integer. Then the ciphertext letter corresponding to m is

$$C = k_m \times 13 \bmod 26 = (2m + 1) \times 13 \bmod 26 = 26 \times +13 \bmod 26 = 13 \bmod 26.$$

m (13) corresponds to M.

An alternative plaintext letter-to-number scheme is

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
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

If this numbering scheme is used, what two letters are fixed by every multiplicative cipher?

Decryption of a Message Encrypted with a Multiplicative Cipher

What undoes multiplication mod 26? Well, division mod 26, but division is just "multiplying by the multiplicative inverse."

Number	1	3	5	7	9	11	15	17	19	21	23	25
Multiplicative inverse	1	9	21	15	3	19	7	23	11	5	17	25

What undoes multiplication by 3 mod 26 is multiplication by 9 mod 26 because $9 \times 3 = 27 = 1 \bmod 26$.

$$\text{plaintext} \xrightarrow{\times 3 \bmod 26} \text{CIPHERTEXT} \xrightarrow{\times 9 \bmod 26} \text{plaintext}$$

Recognition of a Multiplicative Cipher and Its Key by Frequency Analysis

Unlike the Caesar cipher which is easy to recognize by frequency analysis because it translates the frequency patterns, a multiplicative cipher does not preserve the pattern of frequency peaks and valleys that we have with the plaintext alphabet and is, hence, harder to recognize.

Here is a frequency chart for a multiplicative cipher with multiplicative key 7.

Frequencies Multiplicative key = 7

```
A    1111111
B    1111
C    111111
D    1111
E    11
F    1111
G    1111111
H    111
I    1111111111111
J    111111111
K    1111111
L
M    111
N    1
O
P    111
Q    111
R
S    11
T    11111111
U    111
V    11111111
W    11
X    1
Y
Z
```

There are peaks and valleys which correspond to high frequency and low frequency letters and which reflect that a simple substitution cipher was used, but they are not arranged as they are for plaintext. We describe the rearrangement of the patterns of letter frequencies by saying that the alphabet has been **decimated**. The procedure of taking letters at a constant interval apart is called **decimation**. When the multiplicative key is 7, the ciphertext alphabet begins with the seventh letter G and takes every seventh

letter after that, cycling as necessary. We say that the **decimation interval** is 7.

But, based upon the frequency chart, we can often spot a multiplicative cipher and determine the decimation interval, which corresponds to the multiplicative key. Here are some ways to recognize a multiplicative cipher and determine the decimation interval.

Keep in mind that (when we use our plaintext letter-to-number scheme a = 1, … , z = 26) a multiplicative cipher always fixes the letters m and z; In particular, we will use that z is fixed by any multiplicative cipher.

Recall that at the end of the plaintext alphabet there is a string of six low frequency letters – uvwxyz. Their plaintext frequencies look like

u	111	(not high)
v	1	(low)
w	11	(low)
x		(low)
y	11	(low)
z		(low)

So, if we begin with ciphertext Z (which must correspond to plaintext z) and count backwards one decimation interval, we should arrive at another low frequency letter. Then another. And another. Etc. Six in a row.

For example, consider the frequencies that correspond to a multiplicative key of 7.

```
A    1111111
B    1111
C    111111
D    1111
E    11              *
F    1111
G    1111111
H    111
I    1111111111111
J    111111111
K    1111111
L                    *
M    111
N    1               *
O                    *
P    111
Q    111
R                    *
S    11              *
T    11111111
U    111
V    11111111
W    11              *
X    1               *
Y                    *
Z                    *
```

Begin with Z which we know to correspond to plaintext z. The decimation interval must be one of 1 (which would yield the plaintext alphabet), 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, or 25. Try each of these intervals one at a time counting backwards, cycling as needed, from Z until we find a decimation interval that results in six low frequency letters in sequence.

k_m =				
	3	Z (low)	W (low)	T (high)
	5	Z (low)	U (high)	
	7	Z (low)	S (low)	L (low)
		E (low)	X (low)	Q (not high)

This seems to work. The decimation interval – the key -- appears to be 7, and it is.

Notice that the pattern of frequencies suggests that I = e. It is only necessary to determine one correspondence between a plaintext and

ciphertext letter to determine the key. The frequency patterns suggest that `I` = `e`; so, $9 = 5 \times k_m \bmod 26$, where k_m is the multiplicative key.
Divide both sides of the congruence by 5. Dividing means to multiply by the multiplicative inverse.

Number	1	3	5	7	9	11	15	17	19	21	23	25
Multiplicative inverse	1	9	21	15	3	19	7	23	11	5	17	25

We need to multiply both sides of the congruence by 21.

$$k_m = 21 \times 9 \bmod 26 = 189 \bmod 26 = 7 \bmod 26$$

The multiplicative key is 7.

Cryptanalysis by Brute Force

There are even fewer multiplicative ciphers than Caesar ciphers. So, if we knew that a message were encrypted with a multiplicative ciphers, a brute force attack would be reasonable.

Here is a ciphertext message that is known to have been encrypted with a multiplicative cipher.

```
JDIHA   ICDGB   JAPKT   BAQJJ   DIEKV   KTWAP
JDITI   EVAJA   VCOQK   UYFSG   TBJDI   SEIVI
FQUYS
```

The key space is very small, so it is reasonable to try applying each of the 12 inverses to each of the letters of the first five-letter block if the ciphertext and look for something that makes sense.

m	m^{-1}	J	D	I	H	A	JDIHA
1	1	10	4	9	8	1	jdiha
3	9	12	10	3	20	9	ljcti
5	21	2	6	7	12	21	bfglu
7	15	20	8	5	16	15	thepo
9	3	4	12	1	24	3	dlaxc
11	19	8	24	15	22	19	hxovs
15	7	18	2	11	4	7	rbkdg
17	23	22	14	25	2	23	vnybw
19	11	6	18	21	10	11	frujk
21	5	24	20	19	14	5	xtsne
23	17	14	16	23	6	17	npwfq
25	25	16	22	17	18	25	pvqry

$m = 7$ appears to be correct.

Cryptanalysis Using a Known Plaintext Attack

We could also search through the message for an encrypted version of `the`.

```
JDIHA   ICDGB   JAPKT   BAQJJ   DIEKV   KTWAP
JDITI   EVAJA   VCOQK   UYFSG   TBJDI   SEIVI
FQUYS
```

Here is the word `the` encrypted using all 12 possible multiplicative keys.

k_m	
1	THE
3	HXO
5	VNY
7	JDI
9	XTS
11	LJC
15	NPW
17	BFG
19	PVQ
21	DLA
23	RBK
25	FRU

At the very beginning of the ciphertext, we find `JDI` which corresponds to `the` when the multiplicative key is 7.

Exercises

```
01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
 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
```

1. Construct a plaintext-ciphertext correspondence for a multiplicative cipher with multiplicative key 11. Also write the disjoint cycles for the key.

2. Encrypt the following message using a multiplicative cipher with multiplicative key 11.

```
The Adventure of the Dancing Men
```

3. Use frequency analysis to cryptanalyze the following ciphertext:

```
IBWGV   GFFIT   HAICC   JAVSJ   DWAFB   NQWPG
CUKTG   JIBDK   MEDIT   DIEGC   IKWDJ
```

4. Use brute force by applying each of the 12 inverses to the letters of the first five-letter block of the following ciphertext:

```
CMSPU   HXOVA   SPOOB   EAPCO   BACJO   EVASP
CUOQC   EJAOK   HOPCP   HUOPO   BCJJO   QCJJO
PDKPA   SB
```

5. Search through the following ciphertext (which was encrypted with a multiplicative cipher) and find an encrypted version of the word `the`. Then determine the multiplicative key and recover the plaintext.

```
XTSVI    XCEVI    DOSAG    FCXQI    KSVAQ    COXTS
DIFKS    OXIVJ    NEXSV    XCIDD    QMEOX    CVXFG
OCPSI    MSFCA    IVCVX    SDDCK    SVASI    KSVAQ
```

6. Find a word (of more than one letter) and a multiplicative cipher that encrypts that word as another word.

7. If GMSY are consecutive letters in the ciphertext alphabet of a multiplicative cipher, what is the decimation interval?

8. Try to determine the decimation interval from the following frequency chart by search backwards from Z for a string of six low frequency letters.

```
A    111
B    111
C
D    111
E    1111111
F    1
G
H    1111
I    11
J    1
K    11
L    11111111
M    111
N    1111
O    111
P
Q    111111
R    11111111
S    1111111
T    1111
U    11
V    111111111
W    1111111
X
Y    1111111111111
Z
```

9. If 12 is used as a multiplier, how many plaintext letters correspond to each ciphertext letter? If 15 is used?

10. An alternative plaintext letter-to-number scheme is

```
00  01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
 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
```

If this numbering scheme is used, what two letters are fixed by every multiplicative cipher?

11. For each of the twelve possible multiplicative cipher keys, determine the disjoint cycles representation of the key. Explain the pattern.

12. A message is known to be encrypted with a multiplicative cipher. We suspect that plaintext `e` corresponds to ciphertext `G`. What is the multiplicative key? Repeat the exercise with plaintext `e` corresponding to ciphertext `A`.

13. A Multiplicative cipher has a multiplicative key of 11. To what ciphertext letter does plaintext `h` correspond? To what ciphertext letter does plaintext `n` correspond?

14. A multiplicative cipher has a multiplicative key of 9. To what ciphertext letter does plaintext `t` correspond?

14. A message is known to be encrypted with a multiplicative cipher. If plaintext `e` corresponds to ciphertext `O`, what is the multiplicative key? To what ciphertext letter would plaintext `d` correspond?

15. A message is known to be encrypted with a multiplicative cipher. If plaintext `e` corresponds to ciphertext `G`, what is the multiplicative key? To what ciphertext letter would plaintext `l` correspond?

17. If a message is first encrypted with a multiplicative cipher having multiplicative key 7 and then encrypted again with a multiplicative cipher having multiplicative key 19, what is the composed cipher?

18. What is the effect of encrypting a message using a multiplicative cipher with a multiplicative key of 5 and then encrypting again with an multiplicative key of 15?

19. If a message is first encrypted with a multiplicative cipher having multiplicative key 19 and then encrypted again with a multiplicative cipher having additive key 11, what results?

20. If a message is first encrypted with a multiplicative cipher and then encrypted again with a multiplicative cipher, is security increased? Explain.