Spring 2015
Chris Christensen
MAT/CSC 483

Affine Ciphers

Composed Ciphers

Sometimes ciphers are composed in an effort to enhance security, but security might not be enhanced.

Consider encrypting a message twice with Caesar ciphers. Let's say the message was first encrypted using a Caesar cipher with additive key 7 and then was re-encrypted using a Caesar cipher with additive key 11. Was security enhanced? No, the result of composing the two ciphers is equivalent to having encrypted the message once using a Caesar cipher with additive key 18.

Consider encrypting a message twice with multiplicative ciphers. Let's say the message was first encrypted using a multiplicative cipher with multiplicative key 3 and then was re-encrypted using a multiplicative cipher with multiplicative key 7. Was security enhanced? No, the result of composing the two ciphers is equivalent to having encrypted the message once using a multiplicative cipher with multiplicative key 21.

In neither of these cases is the security enhanced by re-encryption – by composing two ciphers.

That is because both the set of Caesar ciphers and the set of multiplicative ciphers form (mathematical) groups under composition. A (mathematical) **group** is a set with an operation (i.e., a way of combining elements), that has four properties – the operation is closed, the operation is associative, there is an identity for the operation, and each element of the set has an inverse for the operation. For the group of Caesar ciphers, the elements of the group are the 26 Caesar ciphers and the operation is composition – combining two encryptions by doing one encryption after the other. The operation being *closed* means that when two elements of the group are combined the result is another element of the group. For example, when re-encrypting a Caesar cipher with additive key 7 using a Caesar cipher with additive key 11, the result is a Caesar cipher with additive key 18. An *identity* is an element that "does nothing." For the group of Caesar ciphers, the identity is the Caesar cipher with additive key 0; this cipher leaves messages unchanged. The *inverse* of an element is the element that "undoes" what the element "does." For example, the inverse of the Caesar cipher with additive key 8 is the Caesar cipher with additive key 18 because the result of encrypting first using a Caesar cipher with one of these keys and then re-encrypting with a Caesar cipher using the other key is the Caesar cipher with additive key 0 – the identity. *Associativity* is the usual algebraic property that permits an operation to be extended to more than two elements. Let's say, we want to encrypt a message three times: once with a Caesar cipher with additive key 5, next with a Caesar cipher with an additive key 9, and finally with a Caesar cipher with additive key 11. Remember that we can only compose two ciphers at a time. Associativity says that we could do this three-step encryption in two equivalent ways:

> We could encrypt using the first key and re-encrypt using the second key and then re-encrypt that result using the third key$\left(\mathrm{p}\xrightarrow{+5}\mathrm{C}_1\xrightarrow{+9}\mathrm{C}_2\right)\xrightarrow{+11}\mathrm{C}$ which is equivalent to $\left(\mathrm{p}\xrightarrow{+14}\mathrm{C}_2\right)\xrightarrow{+11}\mathrm{C}$,
>
> Or we could re-encrypt the second key by the third key and re-encrypt the first encryption by that result $\mathrm{p}\xrightarrow{+5}\mathrm{C}_1\left(\xrightarrow{+9}\mathrm{C}_2\xrightarrow{+11}\mathrm{C}\right)$ which is equivalent to $\mathrm{p}\xrightarrow{+5}\mathrm{C}_1\left(\xrightarrow{+20}\mathrm{C}\right)$.

Associativity means that we need not worry about how we group ciphers when we compose them. Notice that associativity says nothing about commutativity – the order of doing the operations. Being a group does not require commutativity.

The group of multiplicative ciphers has 12 elements and the operation is composition – re-encryption. The operation is closed; for example, when re-encrypting a multiplicative cipher with multiplicative key 3 using a multiplicative cipher with multiplicative key 21, the result is a multiplicative cipher with multiplicative key 11. The identity is the multiplicative cipher with multiplicative key 1 because this cipher leaves the message unchanged. Each multiplicative cipher has an inverse; for example, the inverse of the multiplicative cipher with additive key 15 is the multiplicative cipher with additive key 7 because the result of encrypting first using a multiplicative cipher with one of these keys and then re-encrypting with a multiplicative cipher using the other key is the multiplicative cipher with additive key 1 – the identity. Again, re-encryption is associative.

Security is not enhanced when re-encryption is done by two elements from the same group – the result is just another element from that group. What took two steps could have been done in one.

Security can, however, be enhanced by encrypting first with a cipher from one group and then re-encrypting using a cipher that is not in that group. For example, security can be enhances by encrypting first with a multiplicative cipher and then by a Caesar cipher (or vice versa). Such encryption is called an affine cipher. What took two steps really requires two steps.

Cryptography of Affine Ciphers

Caesar ciphers and the multiplicative ciphers can be combined in two ways:

> We could first encrypt using a multiplicative cipher with multiplicative key *m* and then re-encrypt with a Caesar cipher with additive key *b*. This results in $\mathrm{C} = m\mathrm{p} + b$ where p is plaintext and C is ciphertext.
>
> Or, we could first encrypt using a Caesar cipher with additive key *b* and then re-encrypt with a multiplicative cipher with multiplicative key *m*. This results in $\mathrm{C} = m(\mathrm{p} + b)$.

Either of these methods is called an **affine cipher**.

These two methods typically do not yield the same ciphertext. For example, if we begin with plaintext b (= 2), encrypt with a multiplicative cipher with multiplicative key 5, and re-encrypt with a Caesar cipher with additive key 12; we obtain ciphertext V ($5 \times 2 + 12 = 22 \bmod 26$). But, if we first encrypt b with a Caesar cipher with additive key 12 and then re-encrypt with a multiplicative cipher with multiplicative key 5; we obtain ciphertext R ($5 \times (2 + 12) = \bmod 26$).

We will agree to always do the multiplicative cipher first, and we will number the alphabet a = 01, …, z = 26.

Notice that the formula for encryption $\mathrm{C} = m\mathrm{p} + b$ looks like the equation for a line.

The word "affine" is applied in mathematics to transformations that maintain a "kinship" between the original object and the transformed object. For example, points that are close together should be transformed to points that are also close together. "Affine" comes from the same root word as "affinity." The transformation $\mathrm{x} \to m\mathrm{x}+b$ has this affine property (if two points on the number line x_1 and x_2 are close together, then $mx_1 + b$ and $mx_2 + b$ should also be close together); hence the name for the cipher.

The Size of the Key Space

An affine cipher has two parts to its key – an additive part *b* (the shift) and a multiplicative part *m* (the decimation interval). There are 26 Caesar ciphers; so, there are 26 choices for *b*. For each of those 26 choices for the additive key, there are 12 possible choices for the multiplicative key *m*. Therefore, there are $26 \times 12 = 312$ possible affine ciphers. Of course, one of these is the identity; it does nothing – the cipher with *b* = 0 and *m* = 1 ($\mathrm{C} = 1 \times \mathrm{p} + 0 = \mathrm{p}$), the plaintext alphabet. This would obviously not be a good choice for encryption.

The 312 affine ciphers include, as special cases, the 26 Caesar ciphers (the affine ciphers with *m* = 1: C = p + *b*) and the multiplicative ciphers (the affine ciphers with *b* = 0: C = *m*p).

That's still a small keyspace.

Here is an example of an affine cipher with additive key 5 and multiplicative key 7.

Affine cipher

Multiplicative key = 7 and additive key = 5

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

Shoes and Socks

Usually to encrypt or decrypt using an affine cipher, we would probably construct the plaintext/ciphertext correspondences and make substitutions, but because affine encryption is a two-step process, let’s consider a bit more carefully the decryption process. We have agreed to encrypt using the process $\mathrm{C} = m\mathrm{p} + b$; i.e., first we multiply and then we add. To undo this process – to do the inverse process – we must reverse that order. We first undo the addition (by adding the additive inverse of the additive key), and then we undo the multiplication (by multiplying by the multiplicative inverse of the multiplicative key). Mathematicians sometimes call this the "shoes and socks" principle. It applies to constructing the inverse of a process that is done in steps. The principle is that the inverse process reverses the steps as a person does when removing shoes and socks – when putting on shoes and socks, the socks are put on first and then the shoes are put on; when removing shoes and socks, the shoes are removed first and then the socks. This is an important principle to remember when decrypting a ciphertext that was encrypted in steps.

Enciphering and Deciphering Keys

Caesar ciphers and multiplicative ciphers are affine ciphers. For all three of these ciphers there is a simple, linear algebraic relationship between plaintext and ciphertext.

For Caesar ciphers:

$$\text{CT} = \text{pt} + \text{key} \bmod 26\,.$$

For multiplicative ciphers:

$$\text{CT} = \text{key} \times \text{pt} \mod 26\,.$$

For affine ciphers:

$$\text{CT} = \text{key}_{\text{multiplicative}} \times \text{pt} + \text{key}_{\text{additive}} \mod 26\,.$$

In each case, the enciphering function and the deciphering function are of the same form – only the key differs. For each enciphering key, there is a deciphering key.

For Caesar ciphers, the enciphering function is

$$\text{CT} = \text{pt} + (\text{enciphering key}) \bmod 26\,,$$

and the deciphering function is

$$\text{pt} = \text{CT} + (\text{additive inverse of enciphering key}) \bmod 26\,.$$

The deciphering key is the additive inverse of the enciphering key.

For multiplicative ciphers, the enciphering function is

$$\text{CT} = (\text{enciphering key}) \times \text{pt} \mod 26\,,$$

and the deciphering function is

$$\text{pt} = (\text{multiplicative inverse of enciphering key}) \times \text{CT} \mod 26\,.$$

The deciphering key is the multiplicative inverse of the enciphering key.

Determining the deciphering function from the affine enciphering function is only slightly more complicated. The usual construction of an inverse functions works:

$$\text{CT} = \text{key}_\text{m} \times \text{pt} + \text{key}_\text{a} \mod 26$$

$$\text{CT - } \text{key}_\text{a} = \text{key}_\text{m} \times \text{pt} \mod 26$$

$$(\text{key}_\text{m})^{-1} \times (\text{CT - } \text{key}_\text{a}) = \text{pt} \mod 26$$

$$(\text{key}_\text{m})^{-1} \times \text{CT} + [\text{ - }(\text{key}_\text{m})^{-1} \times \text{key}_\text{a})] = \text{pt} \mod 26$$

$$\text{pt} = (\text{key}_\text{m})^{-1} \times \text{CT} + [\text{ - }(\text{key}_\text{m})^{-1} \times \text{key}_\text{a})] \mod 26\,.$$

The deciphering key is $(\text{k}_m^{-1},\ \text{- }(\text{k}_m^{-1} \times \text{k}_a))$, where k_m is the multiplicative part of the enciphering key and k_a is the additive part of the enciphering key, k_m^{-1} is the multiplicative inverse of k_m modulo 26, and $\text{- }(\text{k}_m^{-1} \times \text{k}_m)$ is the additive inverse of $\text{k}_m^{-1} \times \text{k}_m$ modulo 26.

In each case the deciphering key can easily be determined from knowing the enciphering key.

Modern public key ciphers are two-key ciphers; there is an enciphering key which is public and a deciphering key which is held in private by the receiver of the messages. But, public key ciphers are designed so that just knowing the enciphering key does not permit construction of the deciphering key – an additional piece of information that can be kept secret to the receiver is needed to construct the deciphering key. So, anyone can encipher a message, but only the receiver who holds the deciphering key can read the enciphered message.

Recognition of an Affine Cipher and Its Keys by Frequency Analysis

Just like the multiplicative cipher, an affine cipher with $m \neq 1$ decimates the alphabet but if $b \neq 0$ there is also a shift; therefore, `m` and `z` are not fixed was they would be for a multiplicative cipher.

It is possible to recognize an affine cipher and determine its keys from single letter frequencies if we can spot the decimation interval and the shift.

Here is a frequency chart transformed by the affine cipher with additive key 5 and multiplicative key 7. Notice that there are peaks and valleys of frequencies that are typical of a simple substitution cipher.

Frequencies
Additive key = 5 and Multiplicative key = 7

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

If $b \neq 0$, unlike the multiplicative cipher, ciphertext Z will not correspond to plaintext z. It is much more difficult to determine the decimation interval. By looking at frequencies, we might guess that cipher E corresponds to plaintext z. Then, using the various possible decimation intervals to count backwards from E in search of a string of low frequency characters, we might find that

E	(low)
X	(low)
Q	(low)
J	(low)
C	(low)
V	(not high)

And determine that $b = 5$ and $m = 7$. There are better ways.

Another Cryptanalysis by Frequency Analysis

If single-letter ciphertext frequencies exhibit peaks and valleys, we should suspect that a simple substitution cipher was used.

Let's assume that the method of encryption is an affine cipher.

Recall that for a Caesar cipher $\mathrm{C} = \mathrm{p} + b \mod 26$ we need only one plaintext-ciphertext letter correspondence to determine the additive key *b*, and for a multiplicative cipher $\mathrm{C} = m\mathrm{p} \mod 26$ we need only one plaintext-ciphertext letter correspondence to determine the multiplicative key *m*. One way of cryptanalyzing those ciphers is to assume that the most common ciphertext letter corresponded to the plaintext e. (If that turned out to be an incorrect choice, we would assume that another high frequency plaintext letter corresponded to e, and we would continue this process until the correct key was determined.)

For an affine cipher, we need to determine two keys: the additive key *b* and the multiplicative key *m*. We need two ciphertext-plaintext correspondences to do that.

Consider the ciphertext:

```
OINRF   HORXH   ONAPF   VHLHM   NZOFU   OINAN
GRLZI   PYNJL   HOINM   KVBLY   GMKVB   SFLAG
LAALY   BNRNY   OVHNG   SXPO
```

Here are the single-letter ciphertext frequencies:

A	11111
B	111
C	
D	
E	
F	1111
G	1111
H	111111
I	1111
J	1
K	11
L	1111111
M	111
N	1111111111
O	11111111
P	111
Q	
R	1111
S	11
T	
U	1
V	1111
W	
X	11
Y	1111
Z	11

Notice that peaks and valleys of frequencies that characterize a simple substitution cipher. Let us assume that an affine cipher was used. (That's a really good choice!) We need two plaintext-ciphertext correspondences. We might begin by assuming the most frequent ciphertext letter `N` corresponds to plaintext `e` and the second most frequent ciphertext letter `O` corresponds to plaintext `t`. Also `OIN` is the most frequent trigraph (it occurs three times). Therefore, `OIN` is likely to correspond to plaintext `the`, which reinforces the conclusion that ciphertext `N` corresponds to plaintext `e` and that ciphertextext `O` corresponds to plaintextext `t.` (It also suggests that ciphertext `I` corresponds to plaintext `h`.)

If we are correct that ciphertext `N` corresponds to plaintext `e` and ciphertext `O` corresponds to plaintext `t`, we have two congruences that we can solve modulo 26 and determine the multiplicative and additive keys.

$$\mathrm{C}{=}m\mathrm{p}+b \bmod 26$$

If ciphertext `N` (C = 14) corresponds to plaintext `e` (P = 5),
$14 = m5 + b \bmod 26$.

If ciphertext `O` (C = 15) corresponds to plaintext `t` (P = 20),
$15 = m20 + b \bmod 26$.

We have a system of congruences to solve modulo 26.

$$\begin{cases} 14 = 5m + b \bmod 26 \\ 15 = 20m + b \bmod 26 \end{cases}$$

This system of congruences is solved as if it were a system of linear equations. We begin by subtracting the first congruence from the second.

$$1 = 15m \bmod 26$$

To solve for *m* we would like to divide by 15. Instead we multiply by the multiplicative inverse of 15 which is 7.

$$7 \times 1 = 7 \times 15m \bmod 26$$

$$m = 7 \bmod 26$$

So, *m* = 7.

Now substitute this into one of the congruences, say the first.

$$14 = 5 \cdot 7 + b \bmod 26$$

$$14 = 35 + b \bmod 26$$

$$b = -21 \bmod 26$$

$$b = 5 \bmod 26$$

So, if we were correct in our belief that ciphertext `N` corresponds to plaintext `e` and ciphertext `O` corresponds to plaintext `t`, then the additive key is b = 5 and the multiplicative key is m = 7. Next we try decrypting the message assuming that the additive and multiplicative keys that we have found are correct, and we get plaintext. That confirms that the key is correct.

Here are *Mathematica* commands that solve the same system of congruences:

```
In:  Solve[{14 == 5m + b, 15 = 20m + b && Modulus ==26}, {m, b}]

Out:  {{Modulus → 26, m→7, b→5}}
```

Now we would try to decipher the message using key m = 7 and b = 5.

If we only felt confident about one of the correspondences, say we were “pretty sure” that ciphertext `N` corresponds to plaintext `e`, we could at least reduce the number of cases that we needed to consider to something more reasonable than 312. If `N` corresponds to `e`,

$$14 = m5 + b \bmod 26$$

Solving for b,

$$b = 14 - m5 \bmod 26$$

Substituting m = 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25; we would get 12 pairs (m, b): (1, 9), (3, 25), (5, 15), (7, 5), (9, 21), (11, 11), (15, 17), (17, 7), (19, 23), (21, 13), (23, 3), (25, 19). If we were correct that `N` corresponds to `e`, then one of these 12 pairs corresponds to the key (which we know is (7, 5)).

Brute Force

Although it would not be pleasant to do by hand (however, you might be willing to do that if the security of the free world depended upon it), it would not be hard to have a computer print out the 312 possible decipherments and select the one that makes sense.

Known Plaintext Attack

We could assume that the plaintext message contains the word `the` and search the trigraphs of the ciphertext for an enciphered version of `the`. On the next seven pages are the 312 affine ciphers of `the` and the keys to which they correspond.

Trigaph of *the*	Multiplicative key	Additive key
ACJ	15	13
AEF	17	25
AGB	19	11
AIX	21	23
AKT	23	9
AMP	25	21
AOL	1	7
AQH	3	19
ASD	5	5
AUZ	7	17
AWV	9	3
AYR	11	15
BDK	15	14
BFG	17	0
BCH	19	12
BJY	21	24
BLU	23	10
BNQ	25	22
BPM	1	8
BRI	3	20
BTE	5	6
BVA	7	18
BXW	9	4
BZS	11	16
CAT	11	17
CEL	15	15
CGH	17	1
CID	19	13
CKZ	21	25
CMV	23	11
COR	25	23
CQN	1	9
CSJ	3	21
CUF	5	7
CWB	7	19
CYX	9	5
DBU	11	18
DFM	15	16
DHI	17	2
DJE	19	14
DLA	21	0
DNW	23	12
DPS	25	24

DRO	1	10
DTK	3	22
DVG	5	8
DXC	7	20
DZY	9	6
EAZ	9	7
ECV	11	19
EGN	15	17
EIJ	17	3
EKF	19	15
EMB	21	1
EOX	23	13
EQT	25	25
ESP	1	11
EUL	3	23
EWH	5	9
EYD	7	21
FBA	9	8
FDW	11	20
FHO	15	18
FJK	17	4
FLG	19	16
FNC	21	2
FPY	23	14
FRU	25	0
FTQ	1	12
FVM	3	24
FXI	5	10
FZE	7	22
GAF	7	23
GCB	9	9
GEX	11	21
GIP	15	19
GKL	17	5
GMH	19	17
GOD	21	3
GQZ	23	15
GSV	25	1
GUR	1	13
GWN	3	25
GYJ	5	11
HBG	7	24
HDC	9	10
HFY	11	22
HJQ	15	20

HLM	17	6
HNI	19	18
HPE	21	4
HRA	23	16
HTW	25	2
HVS	1	14
HXO	3	0
HZK	5	12
IAL	5	13
ICH	7	25
IED	9	11
IGZ	11	23
IKR	15	21
IMN	17	7
IOJ	19	19
IQF	21	5
ISB	23	17
IUX	25	3
IWT	1	15
IYP	3	1
JBM	5	14
JDI	7	0
JFE	9	12
JHA	11	24
JLS	15	22
JNO	17	8
JPK	19	20
JRG	21	6
JTC	23	18
JVY	25	4
JXU	1	16
JZQ	3	2
KAR	3	3
KCN	5	15
KEJ	7	1
KGF	9	13
KIB	11	25
KMT	15	23
KOP	17	9
KQL	19	21
KSH	21	7
KUD	23	19
KWZ	25	5
KYV	1	17
LBS	3	4

LDO	5	16
LFK	7	2
LHG	9	14
LJC	11	0
LNU	15	24
LPQ	17	10
LRM	19	22
LTI	21	8
LVE	23	20
LXA	25	6
LZW	1	18
MAX	1	19
MCT	3	5
MEP	5	17
MGL	7	3
MIH	9	15
MKD	11	1
MOV	15	25
MQR	17	11
MSN	19	23
MUJ	21	9
MWF	23	21
MYB	25	7
NBY	1	20
NDU	3	6
NFQ	5	18
NHM	7	4
NJI	9	16
NLE	11	2
NPW	15	0
NRS	17	12
NTO	19	24
NVK	21	10
NXG	23	22
NZC	25	8
OAD	25	9
OCZ	1	21
OEV	3	7
OGR	5	19
OIN	7	5
OKJ	9	17
OMF	11	3
OQX	15	1
OST	17	13
OUP	19	25

OWL	21	11
OYH	23	23
PBE	25	10
PDA	1	22
PFW	3	8
PHS	5	20
PJO	7	6
PLK	9	18
PNG	11	4
PRY	15	2
PTU	17	14
PVQ	19	0
PXM	21	12
PZI	23	24
QAJ	23	25
QCF	25	11
QEB	1	23
QGX	3	9
QIT	5	21
QKP	7	7
Qml	9	19
QOH	11	5
QSZ	15	3
QUV	17	15
QWR	19	1
QYN	21	13
RBK	23	0
RDG	25	12
RFC	1	24
RHY	3	10
RJU	5	22
RLQ	7	8
RNM	9	20
RPI	11	6
RTA	15	4
RVW	17	16
RXS	19	2
RZO	21	14
SAP	21	15
SCL	23	1
SHE	25	13
SGD	1	25
SIZ	3	11
SKV	5	23
SMR	7	9

SON	9	21
SQJ	11	7
SUB	15	5
SWX	17	17
SYT	19	3
TBQ	21	16
TDM	23	2
TFI	25	14
THE	1	0
TJA	3	12
TLW	5	24
TNS	7	10
TPO	9	22
TRK	11	8
TVC	15	6
TXY	17	18
TZU	19	4
UAV	19	5
UCR	21	17
UEN	23	3
UGJ	25	15
UIF	1	1
UKB	3	13
UMX	5	25
UOT	7	11
UQP	9	23
USL	11	9
UWD	15	7
UYZ	17	19
VBW	19	6
VDS	21	18
VFO	23	4
VHK	25	16
VJG	1	2
VLC	3	14
VNY	5	0
VPU	7	12
VRQ	9	24
VTM	11	10
VXE	15	8
VZA	17	20
WAB	17	21
WCX	19	7
WET	21	19
WGP	23	5

WIL	25	17
WKH	1	3
WMD	3	15
WOZ	5	1
WQV	7	13
WSR	9	25
WUN	11	11
WYF	15	9
XBC	17	22
XDY	19	8
XFU	21	20
XHQ	23	6
XJM	25	18
XLI	1	4
XNE	3	16
XPA	5	2
XRW	7	14
XTS	9	0
XVO	11	12
XZG	15	10
YAH	15	11
YCD	17	23
YEZ	19	9
YGV	21	21
YIR	23	7
YKN	25	19
YMJ	1	5
YOF	3	17
YQB	5	3
YSX	7	15
YUT	9	1
YWP	11	13
ZBI	15	12
ZDE	17	24
ZFA	19	10
ZHW	21	22
ZJS	23	8
ZLO	25	20
ZNK	1	6
ZPG	3	18
ZRC	5	4
ZTY	7	16
ZVU	9	2
ZXQ	11	14

It could be an unpleasant experience to compare one-by-one all of the trigraphs of the ciphertext against the table, but we luck out. The very first trigraph `OIN` appears in the table as the enciphered version of `the` when the multiplicative key is 7 and the additive key is 5.

Of course, software can be constructed to determine trigraph frequencies. Using CryptoMIGHT a program written (2003) by NKU students John Rasp, Adam Moore, and Kevin Mooreland or Vbreaker written by Amber Rogers (2008), we would find that there are only three ciphertext trigraphs that appear more than once: `OIN` appears 3 times, `MKV` appears 2 times, and `KVB` appears 2 times.

A more sophisticated approach using single-letter frequencies would be to make a collection of 312 frequencies tables by taking the frequencies for plaintext and apply the 312 affine transformations to the plaintext letters. Then, given a ciphertext message, we could determine the ciphertext frequencies and compare them against the tables to determine the best match and, hence, the key.

The Affine Ciphers Are a Group

Composing an affine cipher with another affine cipher does not increase security because the set of affine ciphers is a group. Notice that if we first encrypt plaintext using an affine cipher with key $\left(m_1, \quad b_1\right)$ and then encrypting the ciphertext using an affine cipher with key $\left(m_2, \quad b_2\right)$ is equivalent to enciphering plaintext with an affine cipher with key$\left(m_2 m_1, \quad m_2 b_1 + b_2\right)$:

$$m_2\left(m_1 \times \text{plaintext} + b_1\right) + b_2 = m_2 m_1 \times \text{plaintext} + \left(m_2 b_1 + b_2\right).$$

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

inverses

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

1. Construct a plaintext-ciphertext correspondence for an affine cipher with multiplicative key 11 and additive key 16.

2. Encrypt the following message using an affine cipher with multiplicative key 11 and additive key 16.

```
The Russians and Germans also solved PURPLE.
```

3. Decrypt the following message that was encrypted using an affine cipher with additive key 9 and multiplicative key 7.

```
povqt rqreu bgveh prnnu gbhhq vehul ygtrj uotht
gxree rirqt ehvxr fvsot gmvqq djelw remov nnura
aplgj vehve rntfu vlela yqtuf oqtds rgjnf leitg
utmnu ryqtn jelpe rnuot fluur htptg toriv ehxlg
tnbff tnnpv uouot tevhx rfvso tgbnt myduo tvurq
vreer id
```

4. Use frequency analysis to cryptanalyze the following ciphertext – try to determine the ciphertext letters that correspond to plaintext `e` and `t` and solve the congruences to determine the key:

```
EJURB   IOJMR   XGEMH   HUBXW   TWJZM   QEJUR
BISUS   BWQEI   QVGZW   NBCIV   GZMJU   YWUSB
JWMQS   WHWEB   JIZGE   MHHUB   IOWZW   JMBWM
BXGJN   YWUSB   JWMQ
```

5. Search through the following ciphertext that is known to have been encrypted using an affine cipher for an encrypted version of `the`. Then determine the multiplicative and additive keys and recover the plaintext.

```
yrmdu damnl ntahy ycdpe rnyhy cdeqt ythcc nmyrb
arxxc dqdyc dfxdq dnhmt vycdp amdqx nydqh rpmqn
altal hfhyd jvrps mmdyd vyhpe jdqld mhpej nqtad
hxtyc tancn sujts drang dqnld
```

6. Cryptanalyze the following message that is known to have been encrypted with an affine cipher.

```
dbupc zctyh gldcp ctgsd sbucj ujngd ohmpq kahiu
jmpbo dumqb dsucd ujcdy buclk aajup jusis dbugs
lupdd bumhd meuqo ussmp qcdla ssmnt uyhmn staai
mpqfa htaal scpjd usdmp qdbue apdbu naenu s
```

7. If a message is first encrypted with an affine cipher with additive key 5 and multiplicative key 11 and then encrypted again with an affine cipher having additive key 12 and multiplicative key 3, what results?

8. If a message is first encrypted with an affine cipher with additive key 17 and multiplicative key 19 and then encrypted again with an affine cipher having additive key 21 and multiplicative key 11, what results?

9. A message is encrypted using an affine cipher where $\mathrm{C} = m\left(\mathrm{p} + b\right)$ and the multiplicative key was $m = 7$ and the additive key was $b = 9$. Our method for an affine cipher is $\mathrm{C} = m\mathrm{p} + b$. What are m and b for our method?

10. If we use our method $\mathrm{C} = m\mathrm{p} + b$ with an additive key $b = 9$ and multiplicative key $m = 7$ to encrypted a message, what are the corresponding keys for the method $\mathrm{C} = m\left(\mathrm{p} + b\right)$.