Module 10.4: Exploring Some Historical Ciphers

Gregory V. Bard

January 30, 2020

- This is a practice workbook the Affine Cipher, touching on some shift ciphers (such as the Caesar cipher, the ROT-13 cipher), the Atbash cipher, and the Vigenère Cipher.
- The Affine Cipher was introduced in Module 10-2: The Basics of Modular Arithmetic, and some skills from Module 10-3: Modular Inverses are needed.
- There is a with-answers version, and a without-answers version.
- In the with-answers version of this workbook, the black ink represents the question, and the blue ink represents the answer.

Question 10-4-1

Suppose Boris normally communicates with his handlers in Moscow using the affine cipher, and the encryption function $c = f_B(p) = 7p + 20 \mod 26$, while Natasha normally uses $c = f_N(p) = 11p + 8 \mod 26$. They have a very secret message to send back to Moscow, so they're going to encrypt the message twice, for added security.

As you can probably guess, this is equivalent to using the affine cipher only once, but with a different function.

- If Boris encrypts the plaintext first, followed by Natasha second, then what would BAT encrypt to?

  (B, A, T) becomes (1, 0, 19) and encrypts to $(f_B(1), f_B(0), f_B(19)) \equiv (1, 20, 23)$. We encrypt again to $(f_N(1), f_N(20), f_N(23)) \equiv (19, 20, 1)$, which becomes (T, U, B) or TUB.

- If Natasha encrypts the plaintext first, followed by Boris second, then what would BAT encrypt to?

  (B, A, T) becomes (1, 0, 19) and encrypts to $(f_N(1), f_N(0), f_N(19)) \equiv (19, 8, 9)$. We encrypt again to $(f_B(19), f_B(8), f_B(9)) \equiv (23, 24, 5)$, which becomes (X, Y, F) or XYF.

- If Boris encrypts the plaintext first, followed by Natasha second, then what would the equivalent single affine encryption-function be?

  The equivalent function would be

$$\begin{aligned} c &= f_N(f_B(p)) \\ &= f_N(7p+20) \\ &= 11(7p+20)+8 \\ &= 77p+220+8 \\ &= (52+25)p+228 \\ &= (2(26)+25)p+208+20 \\ &\equiv 25p+8(26)+20 \\ &\equiv 25p+20 \end{aligned}$$

  The equivalent function is $c = f_{NB}(p) = 25p+20$. Indeed, this maps (1, 0, 19) directly to $(19, 20, 1)$. (Feel free to check that yourself.)

- If Natasha encrypts the plaintext first, followed by Boris second, then what would the equivalent single affine encryption-function be?

  The equivalent function would be

$$\begin{aligned} c &= f_B(f_N(p)) \\ &= f_B(11p+8) \\ &= 7(11p+8)+20 \\ &= 77p+56+20 \\ &= (52+25)p+76 \\ &= (2(26)+25)p+52+24 \\ &= 25p+2(26)+24 \\ &= 25p+24 \end{aligned}$$

  The equivalent function is $c = f_{BN}(p) = 25p+24$. We can check by seeing that this maps (1, 0, 19) directly to $(23, 24, 5)$, as desired.

- Is there any added security from encrypting with the affine cipher twice? (Assume we keep the modulus the same, as we did here?)

  Since the double encryption was actually equivalent to a single encryption with some other encryption function, we know that there cannot possibly ever exist any adversary who can break a single affine encryption, yet who cannot break a double affine encryption. More simply, anyone who can break a single affine encryption can also break the double affine encryption, so no security is gained at all.

Question 10-4-2

The ciphertext "URITVUUWT" was encrypted using the affine cipher and the encryption function $c = f(p) = 19p + 21 \bmod 26$. The decryption function has not been provided. One option for recovering the plaintext is to solve equations mod 26. A mathematician would describe this as "solving linear congruence equations."

- To decrypt the letter "U," we must solve the equation $19p + 21 \equiv 20 \bmod 26$. What is the solution to that equation?

  The solution is $p \equiv 15$, which is the plaintext letter "P."

- To decrypt the letter "R," we must solve the equation $19p + 21 \equiv 17 \bmod 26$. What is the solution to that equation?

  The solution is $p \equiv 8$, which is the plaintext letter "I."

- To decrypt the letter "I," we must solve the equation $19p + 21 \equiv 8 \bmod 26$. What is the solution to that equation?

  The solution is $p \equiv 13$, which is the plaintext letter "N."

- To decrypt the letter "T," we must solve the equation $19p + 21 \equiv 19 \bmod 26$. What is the solution to that equation?

  The solution is $p \equiv 4$, which is the plaintext letter "E."

- At this point, we know that the plaintext is "PINE?PP?E." Can you guess the plaintext?

  The plaintext is "pineapple."

As it turns out, this method is inefficient. It is much wiser for us to invert the encryption function. Its inverse will be the decryption function. Here's how we do that:

$$\begin{aligned}
19p + 21 &\equiv c \\
11(19p + 21) &\equiv 11c \\
209p + 231 &\equiv 11c \\
(208 + 1)p + 208 + 23 &\equiv 11c \\
(8(26) + 1)p + 8(26) + 23 &\equiv 11c \\
(0 + 1)p + 0 + 23 &\equiv 11c \\
p + 23 &\equiv 11c \\
p &\equiv 11c - 23
\end{aligned}$$

The decryption function is $p = g(c) = 11c - 23 \bmod 26$, which can also be written as $p = g(c) = 11c + 3 \bmod 26$.

Question 10-4-3

Consider the following three affine encryption functions. Can you find the corresponding decryption function?

By the way, the with-answers version of this workbook has only the final answers for these, not the complete work. However, you can see complete and detailed solutions to 10-4-2 and 10-4-4, which are mathematically similar. Those will explain how to do this problem.

- Each of these is mod 26, by the way.
- What is the decryption function for the encryption function $c = f(p) = 11p + 10$?

  The decryption function is $p = g(c) = 19c + 18$.
- What is the decryption function for the encryption function $c = f(p) = 5p + 16$?

  The decryption function is $p = g(c) = 21c + 2$.
- What is the decryption function for the encryption function $c = f(p) = 23p + 10$?

  The decryption function is $p = g(c) = 17c + 12$.

Question 10-4-4

In Problem 10-2-6, we had the decryption function $p = g(c) = 19c + 17 \bmod 26$, and we used it to decrypt ciphertexts "XTIWVIV" and "VABVILVL" to obtain the plaintext messages "MONTANA" and "ARKANSAS."

Can you compute the encryption function, given that decryption function?

$$\begin{aligned} p &= g(c) \\ p &= 19c + 17 \\ 11p &= 11(19c + 17) \\ 11p &= 11(19)c + 11(17) \\ 11p &= 209c + 187 \\ 11p &= (208 + 1)c + 182 + 5 \\ 11p &= (8(26) + 1)c + 7(26) + 5 \\ 11p &= (0 + 1)c + 0 + 5 \\ 11p - 5 &\equiv c \end{aligned}$$

Therefore the decryption function is $c = f(p) = 11p - 5$ or equivalently $c = f(p) = 11p + 21$, because $-5 + 26 = 21$.

Question 10-4-4$\frac{1}{2}$

Suppose that you capture an enemy agent, and via torture, you manage to extract his decryption function for the affine cipher. It is $p = g(c) = 3c + 14 \bmod 26$. Unfortunately, he died during the interrogation—this does sometimes happen.

You would like to know his encryption function, so that you can forge messages that look as if they came from him. What is his encryption function?

The corresponding encryption function is $c = f(p) = 9p + 4$.

Question 10-4-5

We saw in Question 10-2-7 that the plaintexts "BOATS" and "BEERS" both became "QDDQD." This is a major problem, because someone receiving the ciphertext "QDDQD" won't know if the intended message is BOATS or BEERS. Ciphers that encrypt with an injective function guarantee that each ciphertext has a unique plaintext. (A mathematician would say "one unique pre-image.")

Under what conditions will an affine cipher encryption function

$$c = f(p) = mx + b \bmod N$$

be uniquely decodable?

So long as m is invertible mod N, where N is the modulus, we can compute the decryption function. Of course, if there's a decryption function, then we know the cipher is uniquely decodable, because the decryption function tells us exactly one plaintext. A mathematician would say that for any fixed input, a function always gives the same output.

This means m has to be coprime to N, so that m is invertible mod N. There is no restriction on b.

Question 10-4-6

Let us suppose that while in the shower one morning, you are abducted by Space Aliens. They have posed a cryptography problem for you, to measure the intelligence of the human race. The encryption function isn't given, but the ciphertext is "JNSEGA," and the affine cipher was used. If you don't correctly identify the plaintext from the following choices, then the Space Aliens will destroy the planet. Of course, you have no pencil, no paper, no pen, no calculator, no computer. Nonetheless, it is obvious to you what the answer is—which is it?

Plot twist: even if you cannot answer, if you can narrow it down to two choices, then they'll only blowup Wisconsin.

- A) FRANKFURT
- B) ANTWERP

- C) PARIS
- D) LONDON
- E) READING
- F) ROME
- G) MARSEILLES
- H) PRAGUE
- I) COPENHAGEN
- J) AMSTERDAM

Since the ciphertext is six letters, the plaintext must be six letters, ruling out all answers except LONDON or PRAGUE.

However, LONDON has repeated letters, whereas PRAGUE has each letter being different. The ciphertext has no repeated letters. Therefore, the plaintext cannot have repeated letters. This rules out LONDON, so the answer must be PRAGUE.

Question 10-4-7

If someone encrypts using the affine cipher, changing either m or b will change the ciphertext. Together, (m, b) are called "a key." Modern ciphers have keys too. One reason for using keys is that if the same message is sent more than once (or to different people), if the keys are different, then the ciphertexts will be different, even though the plaintexts are the same.

- How many possible keys are there, working mod 26, for the affine cipher, regardless if the key is uniquely decodable or not?

  There are 26 choices for m and 26 choices for b. Therefore, there are $26^2 = 676$ possible keys. Of course, some of these are spectacularly bad choices, such as $m = 0$. That is one of several reasons why we really should require the key to be uniquely decodable.

- How many possible keys are there, working mod 27, for the affine cipher, regardless if the key is uniquely decodable or not?

  There are 27 choices for m and 27 choices for b. Therefore, there are $27^2 = 729$ possible keys. Again, some of these are spectacularly bad choices, such as $m = 0$.

- How many possible (uniquely decodable) keys are there for the affine cipher if the modulus is 26?

  The choices for m working mod 26 are

$$\{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$$

being the odd members of the integers mod 26, but excluding 13. There are 12 choices of m, and 26 choices of b, so there are $12(26) = 312$ possible keys mod 26.

- How many possible (uniquely decodable) keys are there for the affine cipher if the modulus is 27?

  The choices for m working mod 27 are

  $$\{1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 20, 22, 23, 25, 26\}$$

  being the members of the integers mod 27, except those divisible by 3. There are 18 choices of m, and 27 choices of b, so there are $18(27) = 486$ possible keys mod 27.

Background

Shift ciphers are a very primitive form of encryption. For example, the Caesar cipher was used in the time of Julius Caesar. Encryption was moving the letters backwards three spots in the alphabet. This included the circular wrap around that we would describe as "mod N" today, where N is the length of the alphabet. The ancient Romans had an alphabet very similar to English, but they did not have the letters W, Y, or Z. Furthermore, U and V were the same letter. Also, I and J were the same letter. For simplicity, we'll use the English alphabet. His nephew and successor, Augustus Caesar, used a shift forward of one, instead of three backwards. The Roman historian Suetonius tells us that messages of military significance were encrypted this way!

Another example is `ROT-13`, which was used on internet bulletin boards and newsgroups, primarily to hide offensive jokes, the answers to riddles or puzzles, or sometimes movie reviews that contained spoilers. It protected the answer from a casual glance. Many newsgroup browsers had a feature where you could highlight text, and ROT-13 it.

Problem 10-4-8

Let's practice with these famous shift ciphers.

- Encrypt the plaintext "Suetonius" using the Julius Caesar Cipher. (Encrypting means moving three spots backward in the alphabet.)

  The ciphertext is "PRBQLKF RP."

- Decrypt the ciphertext "PDUBWJBO" using the Augustus Caesar Cipher. (Encrypting means moving one spot forward in the alphabet.)

  The plaintext is "Octavian." Of course, that's the first name that Augustus Caesar was born with.

- Encrypt the plaintext "Suetonius" using the `ROT-13` Cipher. (Encrypting means moving 13 spots forward in the alphabet.)

  The ciphertext is "FHRGBAVHF."

- Encrypt the plaintext "FHRGBAVHF" using the `ROT-13` Cipher.

  The ciphertext is "SUETONIUS."

- Decrypt the ciphertext "XNQPQO" using the Julius Caesar Cipher. (Encrypting means moving three spots backward in the alphabet.)

  The plaintext is "Brutus." Of course, that's the name of Julius Caesar's good friend who stabbed Julius to death (in cooperation with other stabbers).

- Encrypt the ciphertext "HAL" using the Augustus Caesar Cipher. (Encrypting means moving one spot forward in the alphabet.)

  The plaintext is "IBM."

- What movie is the previous subproblem a reference to?

  The movie *2001: A Space Odyssey* included a computer, the HAL-9000, which was an artificial intelligence that became homicidally insane. That movie is connected to a much better book, by Arthur C. Clarke, entitled *2001*. Unusually for such situations, the book and the movie were written simultaneously. I definitely recommend seeing the movie first, and then reading the book second.

Problem 10-4-9

We will continue our exploration of shift ciphers. You might want to refer back to the previous problem.

- How would I represent the Julius Caesar Cipher as an affine function? (Encrypting means moving three spots backward in the alphabet.) Remember to give both an encryption function and a decryption function.

  The encryption function is $c = f(p) = 1p - 3 \bmod 26$ or equivalently $c = f(p) = p + 23 \bmod 26$. The decryption function is $c = f(p) = 1p + 3 \bmod 26$.

- How would I represent the Augustus Caesar Cipher as an affine function? (Encrypting means moving one spot forward in the alphabet.) Remember to give both an encryption function and a decryption function.

  The encryption function is $c = f(p) = 1p + 1 \bmod 26$. The decryption function is $c = f(p) = 1p - 1 \bmod 26$, or equivalently $c = f(p) = 1p + 25$.

- How would I represent the ROT-13 Cipher as an affine function? (Encrypting means moving 13 spots forward in the alphabet.) Remember to give both an encryption function and a decryption function.

  Both the encryption function and the decryption function are "adding thirteen." Formally, we'd write $c = f(p) = p + 13 \bmod 26$, and $p = g(c) = c + 13 \bmod 26$.

A Story from modern times, in Italy

Bernardo Provenzano, the boss of all bosses of the Sicilian mafia (unwisely) used the Caesar cipher until he was arrested in 2006. You might enjoy reading the following news article.

`https://www.theregister.co.uk/2006/04/19/mafia_don_clueless_crypto/`

Problem 10-4-10

We will continue our exploration of shift ciphers. You might want to refer back to the previous two problems. Remember, we're using the 26-letter English alphabet.

- How many possible keys are there, for the shift cipher?

  There are 26 possible shifts, but this includes 0. While the choice of 0 is unwise, it is a valid choice. We have 26 possible encryption functions of the form $c = f(p) = p + k \bmod 26$, where $0 \leq k < 26$ is an integer.

- Does it make sense to encrypt with the shift cipher twice? Why or why not?

  Suppose Alice shifts by k_1 and Bob shifts by k_2. If $k_3 \equiv k_1 + k_2 \bmod 26$, then encrypting with Alice's shift followed by Bob's shift, is equivalent to shifting once by k_3. Also, encrypting with Bob's shift followed by Alice's shift, is equivalent to shifting once by k_3. In any case, no security is gained by encrypting twice, because anyone who can break a single shift-cipher encryption can also break the double shift-cipher encryption.

  It is somewhat noteworthy that "order matters" if encrypting twice with affine ciphers in general. We saw that in exercise 10-4-1, because we had different short-cut encryption functions if Boris encrypted first followed by Natasha, versus Natasha encrypting first followed by Boris. However, if both ciphers are shift ciphers, then the order no longer matters.

- When is the shift cipher uniquely decodable?

  For any fixed shift-value k, any given ciphertext produces exactly one plaintext when decrypted. For this reason, the shift cipher is always uniquely decodable.

Question 10-4-11

The Atbash cipher dates from Ancient Israel, and was used in the text of the biblical prophet Jeremiah, but in many other places also. Whether or not Jeremiah ever actually existed, archeologists agree that Babylon had conquered Ancient Israel in 587 BCE. Some verses critical of the Babylonians could have resulted in punishment. In the Hebrew text, the word for Babylon is encrypted in two places with the Atbash cipher (Jeremiah 25:26 and Jeremiah 51:41), and the word for the Chaldeans is encrypted once (Jeremiah 51:1).

Of course, we'll use English instead of Hebrew. The Atbash cipher has no mathematics at all. It simply involves making some letter substitutions. The first letter of the alphabet is replaced by the last; the second letter with the second last; the third letter with the third last; ...

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

Question 10-4-12

Encrypt these plaintext words with the Atbash cipher:

- Babylon

  The ciphertext is "YZYBOLM."

- Invasion

  The ciphertext is "RMEZHRLM."

Question 10-4-13

Decrypt these ciphertexts with the Atbash cipher:

- RHIZVO

  The plaintext is "Israel."

- QVIFHZOVN

  The plaintext is "Jerusalem."

Question 10-4-14

This one is challenging, but worth thinking about. How would I represent the Atbash Cipher as an affine function?

The operation is clearly $c = f(p) = 25 - p \mod 26$, but this can also be written as $c = f(p) = -1p + 25 \mod 26$, or equivalently $c = f(p) = 25p + 25 \mod 26$.