

# Module 10-4 $\frac{1}{2}$ : Exploring the Vigenère Cipher

Gregory V. Bard

February 18, 2020

This module is meant to provide practice questions for the Vigenère cipher. This cipher is interesting for several reasons. First, it is hard to break by hand without having a fragment of the plaintext, but easy to break with such a fragment. Second, it is breakable with a mathematically elegant approach and a computer, even a very slow one. Third, it will foreshadow an important cipher that is still used today, called “the one-time pad.” (It also foreshadows a cipher called “the running-key cipher,” which was used by CIA in the 1990s.) Fourth, this cipher was used historically, including by the Confederate States of America during the US Civil War (1861–1865).

Since the cipher is simple to use, it is suitable for military conditions. At one time, it was called *le chiffre indéchiffrable*, the undecipherable cipher. An article in *Scientific American* in 1917 claimed it was unbreakable. Fifth, this cipher is so famous that no one can claim to be knowledgeable about mathematical cryptography without understanding it. Though the cipher is named for Blaise de Vigenère (1523–1596), historians are certain that it was invented by Giovan Battista Bellaso, and published in 1553.

- The first six questions are a warm up, to see if you can carry out the basic tasks of encrypting and decrypting with the Vigenère cipher.
  - Questions 1, 2, and 3 ask you to encrypt a plaintext message, with both the plaintext and the key provided.
  - Questions 4, 5, and 6 ask you to decrypt an encrypted message, with both the ciphertext and the key provided.
  - In the past, many of my students have decided to save time by decrypting/encrypting only the first half, or even the first third, of these messages. That can be a good strategy for making sure that you have enough time for the advanced questions.
- Questions 7, 8, and 9 will invite you to think critically about some “weak keys” of the Vigenère cipher.
- Questions 10, 11, 12, and 13 are examples of a form of cryptanalysis called KPA (known plaintext attack).

- Remember, decryption is what the legitimate receiver of a message does to make the encrypted message (the ciphertext) into a readable plaintext message. For the Vigenère cipher, and essentially all ciphers from the Renaissance until today, this done when the key is known.
  - In contrast, cryptanalysis is what someone does when they intercept an encrypted message, and they want to turn the ciphertext into a readable plaintext message, but they do not know the key. They either need to exploit unexpected side information, mathematical weaknesses in the cipher, operator errors, or more often two or more of those.
  - Categories of cryptanalytic methods are called “attacks,” reflecting the military heritage of cryptography. Pure mathematicians have laughed in my face because of my use of this terminology, but that’s the vocabulary actually used by experts, so that’s the vocabulary I will be using.
  - In a known plaintext attack, or KPA, we have a tiny fragment of the plaintext. Often, we know the first few letters or the last few letters of the plaintext message. This fragment is called “a crib.” This not refer to the small bit of furniture that babies sleep in, but instead to “crib sheets.” The term “crib sheet” was 20th century slang for a formula-reference card or note sheet used with permission during a mathematics test.
- Questions 14 and 15 will deal some intermediate-level theoretical questions.
  - Lastly, Question 16 deals with the computation of the index of coincidence. This is an important tool used in the CTO attack (CipherText Only attack) on the Vigenère cipher, as described in Trappe & Washington’s textbook, *Cryptography with Coding Theory*, 2nd edition, in Section 2.3.

A copy of *Le Tableau Vigenère* (the Vigenère table) is given on the last page of this module, for your convenience.

## Question 1

The 2018 Boyceville Invitational for Wisconsin Science Olympiad, Question 11:

Using the key “DIPLOMAT” for the Vigenere cipher, please encrypt the following message:  
 “I will be taking the orient express from Paris to Istanbul on the twelfth.”

Group the ciphertext into clusters of five for easy transmission.

First, we prepare the plaintext by removing the spaces and the punctuation. Leave two blank lines between each line of plaintext. You’ll see why in a few moments.

---

I W I L L B E T A K I N G T H E O R I E N T E X P R E S S F

---

R O M P A R I S T O I S T A N B U L O N T H E T W E L F T H

---

To facilitate encryption, it can be helpful to write the key “DIPLOMAT” over and over again, to fill the second lines.

---

I W I L L B E T A K I N G T H E O R I E N T E X P R E S S F  
D I P L O M A T D I P L O M A T D I P L O M A T D I P L O M

---

R O M P A R I S T O I S T A N B U L O N T H E T W E L F T H  
A T D I P L O M A T D I P L O M A T D I P L O M A T D I P L

---

Now use *Le Tableau Vigenère* (the Vigenère table) to compute the ciphertext. You take the row of the plaintext letter, and the column of the letter from the key. Whatever letter you find in the intersection of that row and column is the ciphertext letter. Following that process, we obtain:

---

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

---

Encrypting yields the ciphertext:

Lastly, we group the ciphertext into clusters of five to obtain a message that can be easily transmitted: LEXWZ NEMDS XYUFH XRZXP BFEQS ZTDGR RHPXP CWETH LAILB NUERV ISSFW XONIS

## Question 2

The 2019 state-level test for New York Science Olympiad, Question 9:

The following message was sent in 1905 by an American oil tycoon to his representative in Cairo. He recently sent a gift to the Khedive of Egypt, and he wants to ask his representative how the gift was liked. The tycoon’s representative wants to use the Vigenère cipher, but doesn’t know how to encrypt. Can you encrypt for him? The keyword is CHARMING. Group the ciphertext into clusters of four for easy transmission.

“The gift was received but liked. Museums here have three thousand year old artifacts. Items from your civil war aren’t very old.”

Following the procedure described in the previous question’s solution, we obtain the following result:

```

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

```

Lastly, we group the ciphertext into clusters of four to obtain a message that can be easily transmitted: VOEX UNGC CZRV OMVB GKBL FVBZ NPKV PUHY GBMJ TMEK JHVV FPEK GAHF GANT FFER DWYJ CYTZ RIPZ UPTV YASX QTYF GZPO XPLN MZNX GUTM QZLU NK

### Question 3

The 2019 state-level test for Wisconsin Science Olympiad, Question 9:

A senior secretary of the British diplomatic mission to Egypt has forgotten how to encrypt with the Vigenère cipher. He wants to send the following plaintext to an old friend who has just been posted to Copenhagen. Can you encrypt it for him? Since they are diplomats, they have prearranged the keyword: PEACEFUL. The ciphertext is to be grouped into clusters of five for easy transmission.

“Hello, Old Chap! How’s Denmark? Egypt is a bit too warm, but the pyramids were well worth seeing. Regards!”

Following the procedures described in the solution of Question 1 the ciphertext becomes: W I L N S T F O R L A R L T Q D S I N O E W E P V C P V M X U M X X T Q S B U C B F U V X M Y A N V A O M I M H T V E Y I Q F H D V T J W J Y T C K R G K F L O H

Lastly, we group the ciphertext into clusters of five to obtain a message that can be easily transmitted: WILNS TFORL ARLTQ DSINO EWEPV CPVMX UMXXT QSBUC BFUVX MYANV AOMIM HTVEY IQFHD VTJWJ YTCKR GKFL O H

### Question 4

The 2018 Boyceville Invitational for Wisconsin Science Olympiad, Question 9:

Here is a message to a British spy in Strasbourg, sent from the home office in London. It was encrypted with the Vigenère cipher, using the keyword “ORANGE.” Please decrypt it.

```

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

```

The ciphertext decrypts to I T H I N K T H E H U N G A R I A N E N G I N E E R  
B U I L D I N G T H E G E R M A N F O R T O N T H E B O R D E R W I T H F R A  
N C E C A N B E B R I B E D S E N D A T H O U S A N D P O U N D S

Clearly the message must be “I think the Hungarian engineer building the German fort on the border with France can be bribed. Send a thousand pounds.”

## Question 5

The 2019 National Science Olympiad test, Question 6:

The following ciphertext has been received from an Italian secret agent who is hiding in a cave in Siberia, near a naval base. He’s waiting for the right moment to install a tap on the base’s internet connection. He’s using the Vigenère cipher, and the keyword is FROZEN. Can you decrypt the message?

NTO MRB YSS KMR AVV NAP TCR HXV XYS QI

The ciphertext decrypts into the plaintext I C A N N O T B E L I E V E H O W C O  
L D I T I S H E R E.

Clearly, the message must be “I cannot believe how cold it is here.”

## Question 6

The 2019 Boyceville Invitational for Wisconsin Science Olympiad, Question 14:

Two particular British diplomats have long had the habit of exchanging messages encrypted with the Vigenère cipher. For ease of transmission, they group their ciphertext into blocks of three. They’re using the keyword FREIGHT. Can you decrypt this message?

YYI GJP WSF XXX LIF IIP OTP JCP NUY AFM MVM AXF NMB NAA JHY MKU AJK  
LWA NAY ZXE UBE ISI QIL WYV E

The ciphertext decrypts into the plaintext T H E Y D I D N O T P R E P A R E H I  
M W E L L F O R H A V I N G T E A W I T H T H E Q U E E N H E T H O U G H T I  
T W O U L D B E I C E D T E A.

Clearly, the message must be “They did not prepare him well for having tea with the Queen. He thought it would be iced tea!”

## Question 7

Suppose that a group of criminals has programmed their own smartphone app for transmitting encrypted messages to each other. Unwisely, they have decided to use the Vigenère cipher, with a six-letter key. (At least they are smarter than Bernardo Provenzano, the boss of all bosses of the Sicilian mafia, who was using the Caesar cipher. See the note between Problem 10-4-9 and Problem 10-4-10, in the Module 10.4: “Exploring Some Historical Ciphers” for details.)

Physical access to the server that contains the app for downloading has been obtained, and this will allow the compiled Java byte-code to be modified. The goal is to change the key so that every cellular provider across Europe, no matter how small, can read every message. Is there a key for the Vigenère cipher, six letters long, that will result in the messages being sent “in the clear,” despite being encrypted? Technical term: such keys are called identity keys.

The key should be changed to “AAAAAA” because encrypting with this six-letter key does absolutely nothing.

## Question 8

Let us suppose that we have a situation like the previous question, but with criminals who are slightly more savvy. They might use TCPDUMP, ethereal, or WireShark to display the packet traffic, just to verify that encryption is actually happening. Therefore, if the app displays plaintext messages, the criminals will notice this and will stop using the app, and use something else instead.

I’m sure that we all agree that shift ciphers are very easy to break. What kinds six-letter of keywords will reduce the Vigenère cipher to a mere shift cipher? This would allow the ciphertxts to be broken by hand.

The key should be the same letter, repeated six times, but in this case, not “AAAAAA.” For example, the key “XXXXXX” encrypts like the Julius Caesar Cipher. (Encrypting means moving three spots backward in the alphabet.) Similarly, the key “BBBBBB” encrypts like the Augustus Caesar Cipher. (Encrypting means moving one spot forward in the alphabet.)

## Question 9

With the previous question in mind, what six-letter key would reduce the Vigenère cipher to the shift cipher called ROT-13? Hint: the plaintext “HELLO” should encrypt to the ciphertxt “URYYB” under this key.

The six-letter key to reduce the Vigenère cipher to the shift cipher called ROT-13 is “NNNNNN.”

## Question 10

The 2019 state-level test for New York Science Olympiad, Question 1:

The following message was sent with the Vigenère cipher. It was sent to London from a British observer attached to a French regiment prior to The Battle of the Somme. The key is unknown, but the first few words are very likely “Hello, Old Chap!” because that’s how the last several plaintexts from this source started. Can you recover the entire plaintext? The ciphertxt has been grouped into clusters of five, for ease of transmission.

MPLXS GQOCT EHYPR DMTQJ UZGWW EAURS GZUFR WCEBM XLQPC ARIZP RURY  
 SEYEU MTNQK MSHIF LLMPB MCGSP TESMS OSRVA LSTRY DQJDM RYJCO GW

First, we should write the known plaintext and the known ciphertext, aligned nicely in a table.

H E L L O O L D C H A P ? ? . . .

M P L X S G Q O C T E H Y P . . .

We will look in the row for H (the first plaintext letter), find an M (the first ciphertext letter), and then look up to find out that we are in column F. That’s the first letter of the key. We will look in the row for E (the second plaintext letter), find a P (the second ciphertext letter), and then look up to find out that we are in column L. We will look in the row for L (the third plaintext letter), find an L (the third ciphertext letter), and then look up to find out that we are in column A. Continue this process until you run out of known plaintext.

H E L L O O L D C H A P ? ? . . .

F L A M E S F L A M E S

M P L X S G Q O C T E H Y P . . .

As you can see, the key is “FLAMES.” Now that we have found the key, we can easily decrypt the ciphertext, just as we already did in Questions 4–6 of this module.

We obtain the plaintext sequence  
 H E L L O O L D C H A P T E R R I B L Y U N C  
 E R T A I N A B O U T N E X T B A T T L E C O N Q U E R I N G T H E M A C H I  
 N E G U N W I T H T H E B A Y O N E T S O U N D S F R I G H T F U L L Y D A N  
 G E R O U S

The plaintext message is: “Hello, Old Chap! Terribly uncertain about next battle. Conquering the machine gun with the bayonet sounds frightfully dangerous.”

## Question 11

The 2019 state-level test for Wisconsin Science Olympiad, Question 1:

Let us imagine that in World War One (1914–1919), this message has been sent from the Czar’s general staff to the Imperial War Cabinet in London, a few days after the conclusion of the Brusilov Offensive (1916). The cipher used is the Vigenère Cipher. You are attempting to perform cryptanalysis. You don’t know the key, yet it is known that the plaintext begins with the phrase “The Brusilov Offensive.” The ciphertext has been grouped in clusters of three for easy transmission. Can you recover the plaintext?

WPW QRN UPO WND FYG UVQ NTH TUI HMF ROL VSB

MAV HMJ BQL JTD MJV XAS CDF GUZ MJT KBN SHL

Using the techniques given in the solution to the previous question, we obtain the ciphertext: T H E B R U S I L O V O F F E N S I V E H A S B E E N C O S T L Y E I G  
 H T H U N D R E D T H O U S A N D M E N W E R E K I L L E D

The plaintext message is “The Brusilov Offensive has been costly: eight hundred thousand men were killed.”

## Question 12

The 2019 state-level test for Ohio Science Olympiad, Question 14:

Let us imagine that in World War One (1914–1919), this message has been sent from the Czar’s general staff to the Imperial War Cabinet in London, a few days after the conclusion of the Brusilov Offensive (1916). The cipher used is the Vigenère Cipher. You are attempting to perform cryptanalysis. You don’t know the key, yet it is known that the plaintext ends with the phrase “The Brusilov Offensive.” The ciphertext has been grouped in clusters of three for easy transmission. Can you recover the plaintext?

HQY WTA WUG ZWS TAQ BVI FSM XPD HZW ZIE NLG PAH  
THT FZQ DAR XOL PJW GTA GIU CKX LHX VIN WCS BXL

Using the techniques given in the solution to Question 10, we obtain the ciphertext: E I G H T H U N D R E D T H O U S A N D M E N W E R E K I L L E D H I S T O R Y W I L L R E M E M B E R T H E B R U S I L O V O F F E N S I V E

The ciphertext message is “Eight hundred thousand men were killed. History will remember the Brusilov Offensive.”

**Historical Note:** By the way, the reason that I chose to make two plaintexts about the Brusilov Offensive is not just because 2019 was the 100-year anniversary of the end of World War One (1914–1919). To a large extent, even among those who consider themselves knowledgeable on military history, this offensive has been forgotten. In contrast, much smaller battles have been remembered.

## Question 13

The 2019 National Science Olympiad test, Question 16:

Below you will find a ciphertext sent by a college student named Percy, doing a study-abroad program in China. He encrypted it with the Vigenère cipher, but he uses a different key for each family member, so the key simply isn’t known at all. However, it is known that he signs all his messages with “Love, Percy.” As you can see, the ciphertext has been grouped into clusters of four for easy transmission. Can you recover the plaintext?

VSAG MBCA WOLQ WFTP DZIH KDLT FRIS UVIC SWSU  
SGCX FOTX FUBJ LJEG QQRD ORES DCVT HSRR Q

Using the techniques given in the solution to Question 10, we obtain the ciphertext: D E A R U N C L E A L B E R T A L L I S S P L E N D I D C H I N A I S F A S C I N A T I N G B U T V E R Y C R O W D E D L O V E P E R C Y

The plaintext message is: “Dear Uncle Albert, All is splendid. China is fascinating but very crowded. Love, Percy.”



## Question 14

How would you write the Vigenère in terms of modular arithmetic? In other words, the goal is to make a faithful mathematical model of the Vigenère cipher, using modular arithmetic.

We can use the standard encoding of the English alphabet into the integers mod 26. The plaintext would be represented by a sequence of members of the integers mod 26,  $p_1, p_2, p_3, p_4, \dots, p_n$ , and likewise the ciphertext,  $c_1, c_2, c_3, c_4, \dots, c_n$ . Of course,  $n$  is just the length of the message. Let the key length be  $\ell$ , and the key would similarly be a sequence of members of the integers mod 26, such as  $k_1, k_2, k_3, k_4, \dots, k_\ell$ .

Encryption would be  $c_i \equiv p_i + k_j \pmod{26}$ , where  $j \equiv i \pmod{\ell}$ , and where  $1 \leq i \leq n$ . Similarly, decryption would be  $p_i \equiv c_i - k_j \pmod{26}$ , where  $j \equiv i \pmod{\ell}$ , and where  $1 \leq i \leq n$ .

## Question 15

One common attack in cryptography is called the “Brute Force Attack.” This phrase means simply guessing all the possible keys, often using a computer cluster and parallel computing. Suppose we want to break the encrypted messages (sent using the Vigenère cipher) of a terrorist group. Further suppose that we assume they might choose hard to guess keys, such as “KQZXJW” or “XRLCZK.”

If we assume that the keys are between 3-letters and 10-letters in length (inclusive), then how many possible keys are there?

Since there are 26 letters in the English alphabet, then the answer is clearly

$$26^3 + 26^4 + 26^5 + 26^6 + 26^7 + 26^8 + 26^9 + 26^{10}$$

which is a geometric progression, with first element  $a = 26^3$  and last element  $z = 26^{10}$ . The common ratio is obviously  $c_r = 26$ . Therefore, the sum is

$$S = \frac{a - c_r z}{1 - c_r} = \frac{26^3 - 26(26^{10})}{1 - 26} = \frac{17,576 - 3,670,344,486,987,776}{-25} = 146,813,779,478,808$$

keys in total. A modern computing cluster can do this in a small amount of time (depending on the size of the cluster and the speed of the microprocessors). However, as recently as the time that I first began teaching (Spring of 2005), this would have been computationally infeasible, at least without a large cash expenditure. Instead, the Vigenère cipher could be broken with far less computing power, by using some mathematical ingenuity.

For completeness, I should note that it might take less time to simply add up the eight integers in the sum

$$26^3 + 26^4 + 26^5 + 26^6 + 26^7 + 26^8 + 26^9 + 26^{10} = 146,813,779,478,808$$

and compute the total using a hand calculator, than it would to look up the formula for the sum of a geometric progression.

## Question 16

Here is a ciphertext message that was encrypted using the Vigenère cipher. Compute the index of coincidence for a shift of three.

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

By the way, the ciphertext is from the 2019 state-level test for Ohio Science Olympiad, Question 12. However, that question did not ask about the index of coincidence. Instead, it asked the participants to decrypt, given the key.

It is necessary that we write the ciphertext out neatly, and then write it out again but shifted by three positions. Then we will count the number of positions where the shifted ciphertext equals the unshifted ciphertext.

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

I count four places where the two strings of letters are equal (1 in the first line, 0 in the second line, and 3 in the third line), so the index of coincidence is 4.

# Le Tableau Vigenère

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