CYBR 493A

Module 4: MAKING PAPER CRYPTOGRAPHY TOOLS
Chapter 1: Cracking Codes with Python
Pages 37 - 47

TOPICS

- What is cryptography?
- Codes and ciphers
- The Caesar cipher
- Cipher wheels Doing cryptography with arithmetic
- Double encryption

- Before we start writing cipher programs, let's look at the process of encrypting and decrypting with just pencil and paper.

  This will help you understand how ciphers work and the math that goes into producing their secret messages.

  In this chapter, you'll learn what we mean by cryptography and how codes are different from ciphers.

  Then you'll use a simple cipher called the Caesar cipher to encrypt and decrypt messages using paper and pencil.

What Is Cryptography?

- Historically, anyone who has needed to share secrets with others, such as spies, soldiers, hackers, pirates, merchants, tyrants, and political activists, has relied on cryptography to make sure their secrets stay secret.
- **Cryptography is the science of using secret codes.**

What Is Cryptography?

nyr N.vNwz5uNz5Ns6620Nz0N3z2v
N yvNwz9vNz5N6l9Nyvr9
y0QNnvNwv tyNz
Nw964N6l9N5vzxys690,N.vN2z5u-
3vNz Nr Ny64v,N.vNt644l5ztr vNz
N 6N6 yv90,Nr5uNz Nsvt64v0N
yvN7967v9 BN6wNr33Q N-m63 rz9v

lNN2 Nuwv,N9,vNNlvNrBN3zyN4vN
N6 Qvv0z6nvN.7N0yv4N 4 zzvNN
vyN,NN99z0zz6wz0y3vv26 9
w296vyNNrrNyQst.560N94Nu5y
rN5nz5vv5t6v63zNr5.
N75sz6966NNvw6 zu0 wtNxs6t
49NrN3Ny9Nvzyl

The text on the left is a secret message that has been **encrypted**, or turned into a secret code. It's completely unreadable to anyone who doesn't know how to **decrypt** it, or turn it back into the original English message.

The message on the right is random gibberish with no hidden meaning

Encryption Vs. Decryption

- Encryption keeps a message secret from other people who can't decipher it, even if they get their hands on the encrypted message.
  - An encrypted message looks exactly like random nonsense.
- Decryption brings the text to life using a key used to translate the encrypted text to an understandable text

Definitions

- A **cryptographer** uses and studies secret codes.
  - Of course, these secret messages don't always remain secret.
- A **cryptanalyst**, also called a *code breaker* or hacker, can hack secret codes and read other people's encrypted messages.
  - This book teaches you how to encrypt and decrypt messages using various techniques.

Codes vs. Ciphers

- Unlike ciphers, codes are made to be understandable and publicly available.
  - Codes substitute messages with symbols that anyone should be able to look up to translate into a message.
- In the early 19th century, one well-known code came from the development of the electric telegraph, which allowed for near-instant communication across continents through wires (Morse Code)

Codes vs. Ciphers

- In contrast with codes, a **cipher** is a specific type of code meant to keep messages secret.
- You can use a cipher to turn understandable English text, called *plaintext*, into gibberish that hides a secret message, called the **ciphertext**. (i.e., Shifrah in Arabic شفره).
- A cipher is a set of rules for converting between plaintext and ciphertext.

Codes vs. Ciphers

- These rules often use a secret key to encrypt or decrypt that only the communicators know.
- In our book, you'll learn several ciphers and write programs to use these ciphers to encrypt and decrypt text.
- But first, let's encrypt messages by hand using simple paper tools.

Title: The Birth of Morse Code

- Early 19th century
- Electric telegraph development
- Near-instant global communication
- Replaced slow horseback letter delivery

Title: Morse Code Basics

- Telegraph limitations: "dot" and "dash" pulses
- Encoding: Translate English to pulses
- Decoding: Translate pulses to English
- Morse code: The code of telegraph and radio communication

Encoding Vs. Decoding

- To convert letters of the alphabet into these dots and dashes, you need an encoding system to translate English to electric pulses.
- The process of converting English into dots and dashes to send over a telegraph is called **encoding**, and the process of translating electric pulses to English when a message is received is called **decoding**

Morse Code Encoding

Table 1-1: International Morse Code Encoding

Letter	Encoding	Letter	Encoding	Number	Er
A	• -	N	- •	1	•
B	- • • •	O	- - -	2	•
C	- • - •	P	• - - •	3	•
D	- • •	Q	- - • -	4	•
E	•	R	• - •	5	•
F	• • - •	S	• • •	6	-
G		T		7	

- The code used to encode and decode messages over telegraphs (and later, radio) was called **Morse code**, as shown in Table 1-1. Morse code was developed by Samuel Morse and Alfred Vail.

The Caesar Cipher

- Named after Julius Caesar (2000 years ago)
- Simple and easy to learn
- Vulnerable to cryptanalysis due to its simplicity
- Valuable as a learning exercise

How the Caesar Cipher Works

- Substitutes each letter by shifting the alphabet
- Example: Caesar shifted the alphabet down by three
  - A becomes D, B becomes E, and so on
  - Handles end-of-alphabet shifts by wrapping around
  - Demonstrating encryption with the Caesar cipher

The Cipher Wheel

- Simplifying Caesar cipher with a cipher wheel
- Two rings with 26 slots each (for a 26-letter alphabet)
- Outer ring represents plaintext alphabet
- Inner ring represents corresponding ciphertext letters
- Inner ring numbered 0 to 25 for encryption key
- Circular shift, key > 25 wraps around (e.g., 26 = 0, 27 = 1)

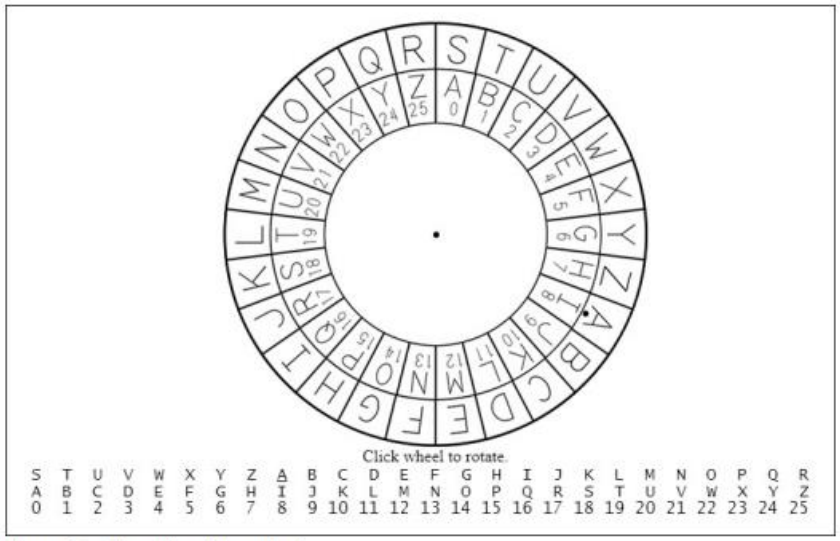

Figure 1-1: The online cipher wheel

Accessing the Virtual Cipher Wheel

- Access the virtual cipher wheel online at https://www.nostarch.com/crackingcodes/
- Figure 1-1 provides a visual representation
- Click and drag to spin the wheel for desired configuration
- Click again to stop the wheel from spinning
- Offers an interactive learning experience

Printable Paper Cipher Wheel

- Printable paper cipher wheel available on the book's website
- Cut out two circles, place smaller in the middle of the larger one
- Insert a pin or brad through the center to spin them
- A hands-on tool for practicing and understanding the Caesar cipher
- Enhances the learning experience

Encrypting with the Cipher Wheel

- To begin encrypting, write your message in English on a piece of paper.
- For this example, we'll encrypt the message THE SECRET PASSWORD IS ROSEBUD.
- Next, spin the inner wheel of the cipher wheel until its slots match up with slots in the outer wheel.
- Notice the dot next to the letter A in the outer wheel.
- Take note of the number in the inner wheel next to this dot. This is the encryption key.

Encrypting with the Cipher Wheel

- For example, in Figure 1-1 (slide 17), the outer circle's A is over the inner circle's number 8.
- We'll use this encryption key to encrypt the message in our example, as shown in Figure 1-2.

T	H	E		S	E	C	R	E	T		P	A	S	S	W	O	R	D		I	S		R	O	S	E	B	U	D
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
B	P	M		A	M	K	Z	M	B		X	I	A	A	E	W	Z	L		Q	A		Z	W	A	M	J	C	L

Figure 1-2: Encrypting a message with a Caesar cipher key of 8

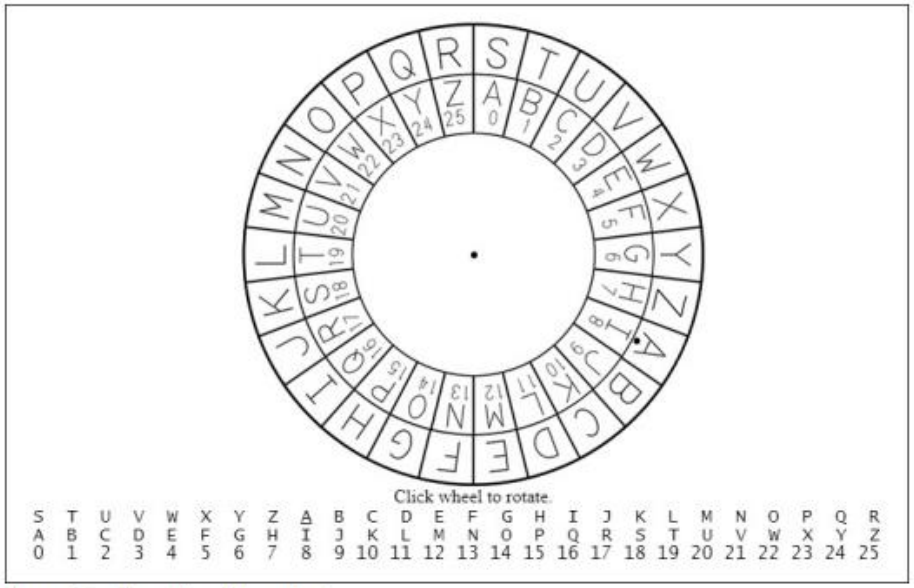

Figure 1-1: The online cipher wheel

T	H	E		S	E	C	R	E	T		P	A	S	S	W	O	R	D		I	S		R	O	S	E	B	U	D
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
B	P	M		A	M	K	Z	M	B		X	I	A	A	E	W	Z	L		Q	A		Z	W	A	M	J	C	L

Figure 1-2: Encrypting a message with a Caesar cipher key of 8

- For each letter in the message, find it in the outer circle and replace it with the corresponding letter in the inner circle.
- In this example, the first letter in the message is T (from "THE SECRET...").
- Locate T in the outer circle and find its corresponding letter in the inner circle, which is B.
- Repeat this process for each letter in the message.

Encrypting with the Cipher Wheel

- Message: THE SECRET PASSWORD IS ROSEBUD
- Encryption Key:
  - T ➔ B
  - H ➔ P
  - E ➔ M
  - (Continue this process for all letters)
- Result: BPM AMKZMB XIAAEWZL QA ZWAMJCL

Encrypting with the Cipher Wheel

- Each letter on the outer wheel always encrypts to the same letter on the inner wheel.
- After determining the encryption for the first occurrence of a letter (e.g., T ➔ B), apply the same encryption for all subsequent occurrences of that letter in the message.
- Non-letter characters, such as spaces, remain unchanged during the encryption process.

Decrypting with the Cipher Wheel

- For example, let's say you receive the ciphertext IWT CTL EPHHLDGS XH HLDGSUXHW and want to decrypt it
- You wouldn't be able to decrypt the message unless you knew the key (or unless you were a
- clever hacker).
  - Luckily, your friend has already told you that they use the key 15 for their messages. The cipher wheel for this key is shown in Figure 1-3 next slide

Decrypting with the Cipher Wheel

- Now you can line up the letter A on the outer circle (the one with the dot below it) over the letter on the inner circle that has the number 15 (which is the letter P).
- Then, find the first letter in the secret message on the inner circle, which is I, and look at the corresponding letter on the outer circle, which is T.
- The second letter in the ciphertext, W, decrypts to the letter H.
- Decrypt the rest of the letters in the ciphertext back to the plaintext, and
- you'll get the message THE NEW PASSWORD IS SWORDFISH, as shown in Figure 1-4 next slide

Figure 1-3: A cipher wheel set to key 15

Decrypting with the Cipher Wheel

I	W	T		C	T	L		E	P	H	H	L	D	G	S		X	H		H	L	D	G	S	U	X	H	W
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
T	H	E		N	E	W		P	A	S	S	W	O	R	D		I	S		S	W	O	R	D	F	I	S	H

Figure 1-4: Decrypting a message with a Caesar cipher key of 15

- If you used an incorrect key, like 16, the decrypted message would be SGD MDV OZRRVNQC HR RVNQCEHRG, which is unreadable.
- Unless the correct key is used, the decrypted message won't be understandable.

Encrypting and Decrypting with Arithmetic

- The cipher wheel is a convenient tool for encrypting and decrypting with the Caesar cipher, but you can also encrypt and decrypt using arithmetic.
- To do so, write the letters of the alphabet from A to Z with the numbers from 0 to 25 under each letter.
- Begin with 0 under the A, 1 under the B, and so on until 25 is under the Z.
- See Figure 1-5 shows what it should look like.

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
0	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

Figure 1-5: Numbering the alphabet from 0 to 25

Encrypting and Decrypting with Arithmetic

- You can use this letters-to-numbers code to represent letters. This is a powerful concept, because it allows you to do math on letters.
- For example, if you represent the letters CAT as the numbers 2, 0, and 19:
  - you can add 3 to get the numbers 5, 3, and 22.
- These new numbers represent the letters FDW, as shown in Figure 1-5 in the previous slide.
- You have just "added" 3 to the word *cat*!
- Later, we'll be able to program a computer to do this math for us.

Encrypting process with Arithmetic

- Use arithmetic to encrypt with the Caesar cipher.
- Find the number under the letter you want to encrypt.
- Add the key number to it.
- The resulting sum is the number under the encrypted letter.

Example Encryption

- Encrypting "HELLO. HOW ARE YOU?" using the key 13.
- Find the number under H (7), add 13: 7 + 13 = 20 (U).
- E (4) + 13 = 17 (R), and so on.
- When the sum exceeds 25, subtract 26 from it.
- O (14) + 13 = 27, 27 - 26 = 1 (B).
- Message: "HELLO. HOW ARE YOU?"
- Result: "URYYB. UBJ NER LBH?"

Decryption Process:

- To decrypt, subtract the key instead of adding it.
- Find the number of the ciphertext letter.
- Subtract the key.
- If the result is less than 0, add 26 to it.

Example Decryption

- Decrypting "URYYB" using the key 13.
- U (20) – 13 = 7 => H …etc
- B (1) - 13 = -12, add 26: -12 + 26 = 14 (O).
- Message: "URYYB"
- Result: "HELLO

- As you can see, you don’t need a cipher wheel to use the Caesar cipher.
- All you need is a pencil, a piece of paper, and some simple arithmetic!

Can we double encrypt with the Ceasar cipher?

- Many people believe that encrypting a message twice with two different keys would double the strength of the encryption. However, this is not the case with the Caesar cipher and most other ciphers.
- Let's explore why double encryption doesn't increase security in the Caesar cipher.

Example 1: Single Encryption

- Encrypt the word "KITTEN" using the key 3.
- Add 3 to the plaintext letter's number.
- Resulting ciphertext: NLWWHQ

Example 2: Double Encryption

- Encrypt "KITTEN" with the key 3, resulting in "NLWWHQ."
- Encrypt "NLWWHQ" with the key 4.
- Add 4 to the plaintext letter's number.
- Resulting ciphertext: RPAALU

- **Observation:**
- The result of double encryption (KITTEN ➔ NLWWHQ ➔ RPAALU) is the same as a single encryption with a key of 7 (KITTEN ➔ RPAALU).
- For the Caesar cipher, and many other ciphers, double encryption does not provide additional strength.
- The result of double encryption can be achieved with a single encryption using a different key.