Cryptography

Chase Wiederstein

2022-10-11

History of Cryptography

Cryptography has been around for centuries and is simply a form of communication. The most simple definition of cryptography is the art of creating and interpreting secret messages. To create a secret message is called “encrypting” and to interpret a secret message is called “decrypting.”

One of the oldest and most famous methods of cryptography is known as the Caeser Cipher. The Caeser Cipher was quite simple. It is just a shifting of the alphabet. First, assign the numbers 0-25 to the alphabet as such.

X0.25 LETTERS 1 0 A 2 1 B 3 2 C 4 3 D 5 4 E 6 5 F 7 6 G 8 7 H 9 8 I 10 9 J 11 10 K 12 11 L 13 12 M 14 13 N 15 14 O 16 15 P 17 16 Q 18 17 R 19 18 S 20 19 T 21 20 U 22 21 V 23 22 W 24 23 X 25 24 Y 26 25 Z

X0.25	LETTERS
0	A
1	B
2	C
3	D
4	E
5	F
6	G
7	H
8	I
9	J
10	K
11	L
12	M
13	N
14	O
15	P
16	Q
17	R
18	S
19	T
20	U
21	V
22	W
23	X
24	Y
25	Z

Then, the encrypter will choose a shift. Suppose the shift is $n = 5$. Each letter in the alphabet will shift 5 units to the right. A will become 5, B will become 6, C will become 7, and so one. Using modular arithmetic, this can be explained using $E_n(x) = x + n(mod 26)$ where x is the original value of the letter and n is the shift value. X0.25 LETTERS 1 0 A 2 1 B 3 2 C 4 3 D 5 4 E 6 5 F 7 6 G 8 7 H 9 8 I 10 9 J 11 10 K 12 11 L 13 12 M 14 13 N 15 14 O 16 15 P 17 16 Q 18 17 R 19 18 S 20 19 T 21 20 U 22 21 V 23 22 W 24 23 X 25 24 Y 26 25 Z

X0.25	LETTERS
0	A
1	B
2	C
3	D
4	E
5	F
6	G
7	H
8	I
9	J
10	K
11	L
12	M
13	N
14	O
15	P
16	Q
17	R
18	S
19	T
20	U
21	V
22	W
23	X
24	Y
25	Z

After encrypting the message and sending it, decrypting it is just as simple. All the receiver needs is the key to unlocking the message, the shifting value, n. To decrpyt, you simply use the function $D_n(x) = x - n(mod 26)$.

Suppose I want to encrpyt the word "CRYPTOGRAPHY" to send to a fellow classmate. Using a shift of $n = 6$, and plugging each individual value of original letter in "CRYPTOGRAPHY" into the encrypting equation, $E_n(x) = n + x(mod 26)$ yields the string of letters "IXEVYUMXGVNE." To decrypt, the fellow classmate will use the key of $n = 6$ allow with the decrypting function $D_n(x) = x - n(mod 26)$ to reverse the shift and read "CRYPTOGRAPHY." However, if the message is intercepted, cracking the encrypted message would take no time at all even without the key. There are only 26 possible combinations of what the shift could be. Over time, this process of creating trickier encryption methods has become much more complex, yet the Caesar Cipher is still a foundational model of how cryptography works.

Introduction

"In ancient India, there were two kinds of ciphers Kauitiliyam and Mulavediya noted in 2000 year old Kamasutra of Vatsyayana." (Naser, 2021, p. 12) (pdf)[1]

"The first cipher device was probably invented by Leon Battista Alberti, an automatic cipher device, where he used a wheel." (Naser, 2021, p. 12) (pdf)[1]

```
## [1] "Hello"
```

Inline link

Rmakrdown Cheatsheet

R Markdown

This is an R Markdown document. Markdown is a simple formatting syntax for authoring HTML, PDF, and MS Word documents. For more details on using R Markdown see http://rmarkdown.rstudio.com.

When you click the **Knit** button a document will be generated that includes both content as well as the output of any embedded R code chunks within the document. You can embed an R code chunk like this:

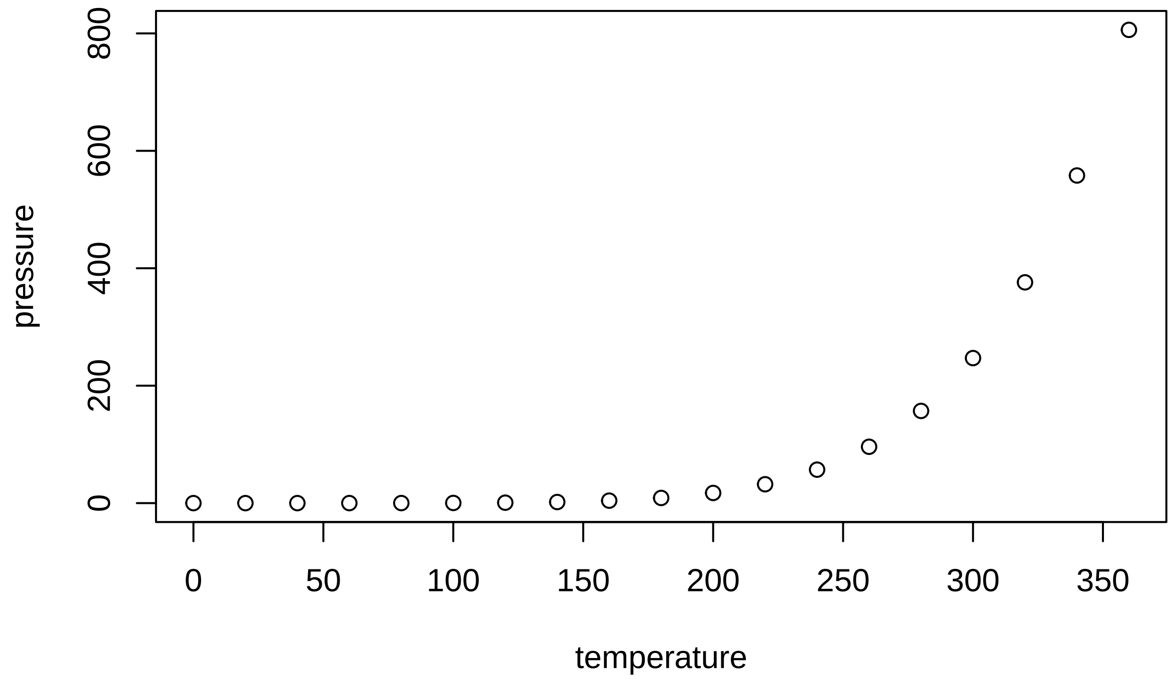
```
summary(cars)
```

```
##      speed           dist       
##  Min.   : 4.0   Min.   :  2.00  
##  1st Qu.:12.0   1st Qu.: 26.00  
##  Median :15.0   Median : 36.00  
##  Mean   :15.4   Mean   : 42.98  
##  3rd Qu.:19.0   3rd Qu.: 56.00  
##  Max.   :25.0   Max.   :120.00
```

```
Hey
```

Including Plots

You can also embed plots, for example:



Note that the `echo = FALSE` parameter was added to the code chunk to prevent printing of the R code that generated the plot.

References

1. Naser SM (2021) Cryptography: From The Ancient History to Now, It's Applications and a New Complete Numerical Model,.