Code Girls: Cryptography

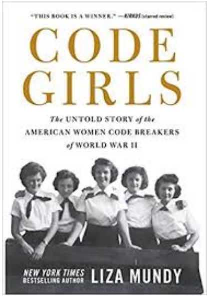
Samantha Allen and Marisabel Rodriguez

Sonia Kovalevsky Day

Dartmouth College

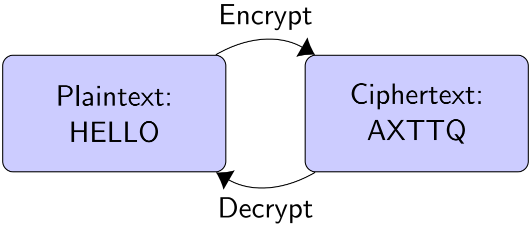
May 11, 2019

Recruited from settings as diverse as elite womens colleges and small Southern towns, more than ten-thousand young American women served as codebreakers for the U.S. Army and Navy during World War II.


"THIS BOOK IS A WINNER." —KIRKUS (starred review)
CODE GIRLS
The UNTOLD STORY of the AMERICAN WOMEN CODE BREAKERS of WORLD WAR II
NEW YORK TIMES BESTSELLING AUTHOR
LIZA MUNDY

Definitions

- **Plaintext** is a message to be communicated.
- **Ciphertext** is a disguised version of a plaintext.
- **Encryption** is the process of turning plaintext into ciphertext.
- **Decryption** is the process of turning ciphertext into plaintext.
- **Cryptology** is the study of encryption and decryption.
- **Cryptography** is the application of cryptology.



First Example: Caesar Cipher

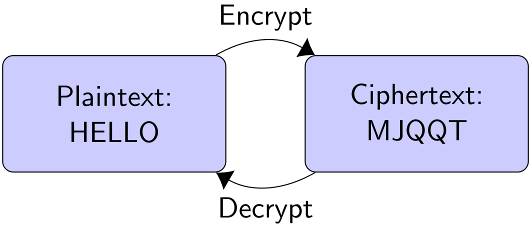
Shift each letter in the alphabet by a fixed number called the **key**.

Example: Key $= 5$

$$\begin{aligned}
A &\xrightarrow{+5} F \\
B &\xrightarrow{+5} G \\
C &\xrightarrow{+5} H \\
&\vdots \\
U &\xrightarrow{+5} Z \\
V &\xrightarrow{+5} A \\
W &\xrightarrow{+5} B \\
&\vdots
\end{aligned}$$

First Example: Caesar Cipher

Plaintext	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
Ciphertext	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



First Example: Caesar Cipher

Alternative approach: Assign each letter a number, add the key to that number, and then switch back to letters.

Letter	A	B	C	D	E	F	···	X	Y	Z
Number	0	1	2	3	4	5	···	23	24	25

$$A \; \Big| \; 0 \xrightarrow{+5} 5 \; \Big| \; F$$

$$X \; \Big| \; 23 \xrightarrow{+5} 28 \; \Big| \; ?$$

First Example: Caesar Cipher

Alternative approach: Assign each letter a number, add the key to that number, and then switch back to letters.

Letter	A	B	C	D	E	F	···	X	Y	Z
Number	0	1	2	3	4	5	···	23	24	25

$$A \mid 0 \xrightarrow{+5} 5 \mid F$$

$$X \mid 23 \xrightarrow{+5} 28 \mid ?$$

In order to "wrap around": find the remainder after dividing by 26.

First Example: Caesar Cipher

Alternative approach: Assign each letter a number, add the key to that number, and then switch back to letters.

Letter	A	B	C	D	E	F	$\cdots$	X	Y	Z
Number	0	1	2	3	4	5	$\cdots$	23	24	25

$$A \mid 0 \quad \xrightarrow{+5} \quad 5 \mid F$$

$$X \mid 23 \quad \xrightarrow{+5} \quad 28 \mid ?$$

In order to "wrap around": find the remainder after dividing by 26.

$$28 \div 26 = 1 \text{ with remainder } 2$$

So the ciphertext for X should be the letter corresponding to 2.

First Example: Caesar Cipher

Alternative approach: Assign each letter a number, add the key to that number, and then switch back to letters.

Letter	A	B	C	D	E	F	$\cdots$	X	Y	Z
Number	0	1	2	3	4	5	$\cdots$	23	24	25

$$A \;\Big|\; 0 \quad \xrightarrow{+5} \quad 5 \;\Big|\; F$$

$$X \;\Big|\; 23 \quad \xrightarrow{+5} \quad 28 \;\Big|\; \mathrm{C}$$

In order to "wrap around": find the remainder after dividing by 26.

$$28 \div 26 = 1 \text{ with remainder } 2$$

So the ciphertext for X should be the letter corresponding to 2.

Notation

If r is the remainder of a when dividing by n, then we write

$$a \equiv r \mod n.$$

“a is congruent to r mod n”

Notation

If r is the remainder of a when dividing by n, then we write

$$a \equiv r \mod n.$$

"a is congruent to r mod n"

For example,

$$28 \equiv 2 \mod 26.$$

Notation

If r is the remainder of a when dividing by n, then we write

$$a \equiv r \mod n.$$

"a is congruent to r mod n"

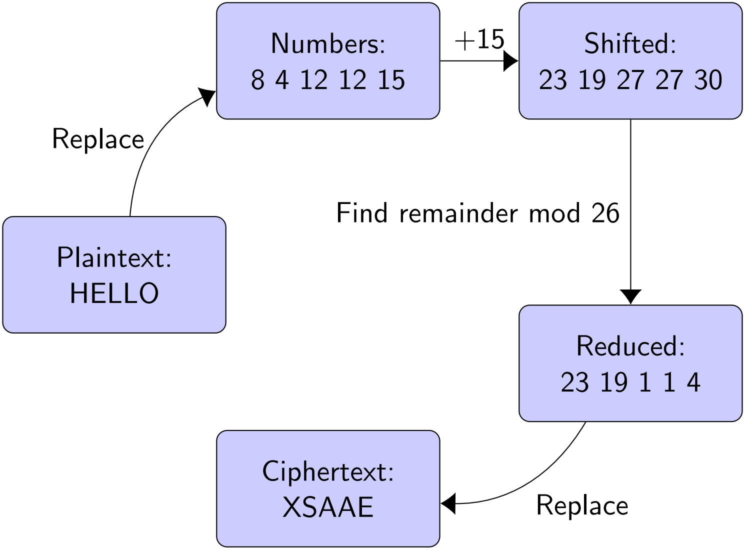
For example,

$$28 \equiv 2 \mod 26.$$

So, if a letter is assigned the number a in 0 through 25, then to find the result of a Caesar cipher with key k we can compute

$$a + k \equiv r \mod 26$$

and the number corresponding to r will be the cipher text.



Plaintext:
HELLO

Replace

Numbers:
8 4 12 12 15

+15

Shifted:
23 19 27 27 30

Find remainder mod 26

Reduced:
23 19 1 1 4

Replace

Ciphertext:
XSAAE

Breakout 1: Encrypt a message.

Each group has been given an envelope. Open that envelope. This is a message that must be kept secret.

Your task: Use a Caesar cipher with a key of your choosing to encrypt the message.

- Choose a key as a group.
- Once you have chosen a key, use division of labor to encrypt the message.
- Be sure to keep the key secret from the neighboring groups.

Decrypting a Caesar cipher

If you know the key?

Decrypting a Caesar cipher

If you know the key? Shift back.

Decrypting a Caesar cipher

If you know the key? Shift back.
Given the encrypted value r, find plaintext value a so that

$$a + k \equiv r \mod 26$$

In other words,

$$(a + k) \div 26 = d \text{ with remainder } r.$$

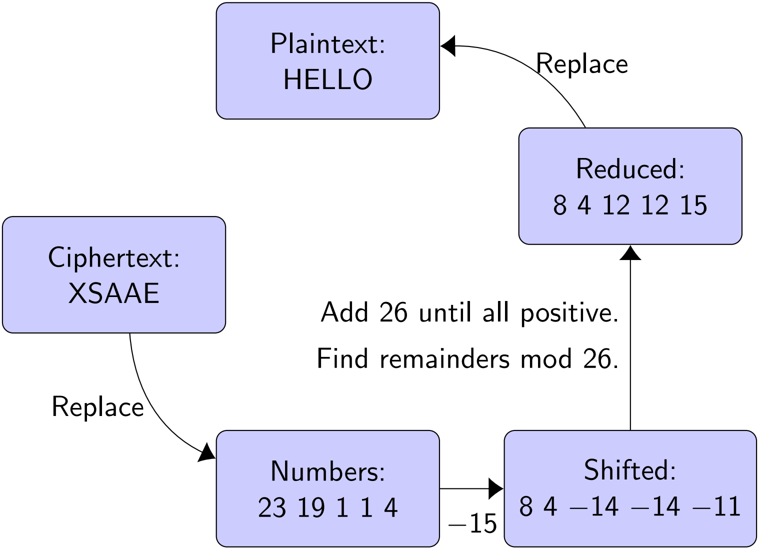
This means

$$a + k = d \times 26 + r$$

$$a - (d \times 26) = r - k$$

So

$$r - k \equiv a \mod 26.$$



Ciphertext:
XSAAE

Replace

Numbers:
23 19 1 1 4

-15

Shifted:
8 4 -14 -14 -11

Add 26 until all positive.

Find remainders mod 26.

Reduced:
8 4 12 12 15

Replace

Plaintext:
HELLO

Decrypting a Caesar cipher

What if you don’t know the key?

Decrypting a Caesar cipher

What if you don't know the key?

- How many different keys are possible?

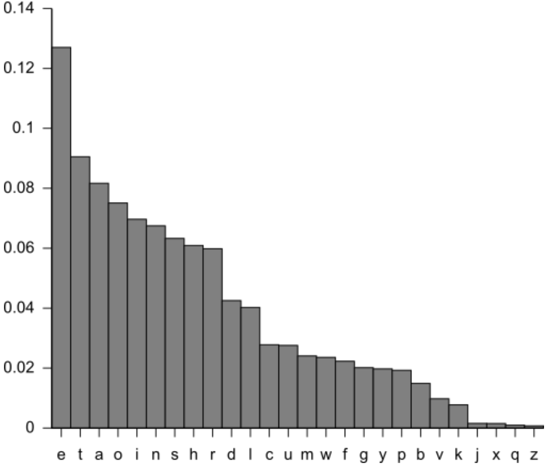
Decrypting a Caesar cipher

What if you don't know the key?

- How many different keys are possible?
- How can we make educated guesses about the key?

Frequency Analysis

Given a sufficiently large block of ciphertext, the frequency of each letter should follow the rules of the English language.



Breakout 2: Intercept a message.

The interceptor's task: Decrypt the message (without the key!).

- Count the number of times each letter appears in the ciphertext. Identify the letters that are most common.
- Use the frequency analysis chart for the English language found in your packets to make a guess about the plaintext corresponding to the most common letter in the ciphertext.
- Identify which key would cause the correct shift of the most common letter.
- Use that key to decrpyt the ciphertext.
- If the result is nonsense, try choosing the key based on the next most common letter in the ciphertext.

Improvements?

Breakout 3: Random substitution cipher.

Each of you has been given a block of encrypted text. Each letter corresponds to a different letter in the English alphabet. However, a Caesar cipher was not used. Each letter was assigned randomly. Use frequency analysis to identify most common letters, and then use context clues to find the plaintext.