LE/EECS 4161 Final Project
The Caesar Cipher

S.Toyonaga
York University

Agenda

- The Pitch
- Mathematical Background
- Historical Applications
- Technical Applications
- Cipher Demo
- Cipher Evaluation

The Pitch

- Caesar Cipher is one of the earliest cryptographic systems to date.
  - Strengths?
  - Weaknesses?
  - How were the Weaknesses Discovered?
- Learning about predecessor ciphers will help you:
  - Develop stronger, more tamper-resistant cipher system(s)
  - Learn how to test / exploit known weaknesses in unknown ciphers

- ***“Those who cannot remember the past are condemned to repeat it.”***

  – George Santayana

Mathematical Background

- Monoalphabetic Substitution Cipher
  - Modular Arithmetic (Wrap-Around)
  - (Modular Factor = Len(Alphabet))
- Key Space: 26
- **Initial Alphabet Representation:**

A	B	C	D	E	F	G	…	Z
0	1	2	3	4	5	6	…	25

- **Encryption**
  - **$(P_i + k) \% 26$**
- **Decryption:**
  - **$(C_i - k) \% 26$**

Historical Applications

1. **A Solution to Hair ⇒ Message Steganography**
    a. Shave a Slaves Head
        i. Write a Message onto it
        ii. Wait for Hair to Regrow
    b. Send the Slave (Ciphertext) to the message receiver for re-shaving

Historical Applications

2. Secret Messages

a. Sent private letters to friends and highly ranking officials on the battlefield.

b. Documented in use as early as 50 B.C., with Julius Caesar writing to Marcus Cicero

c. Original System

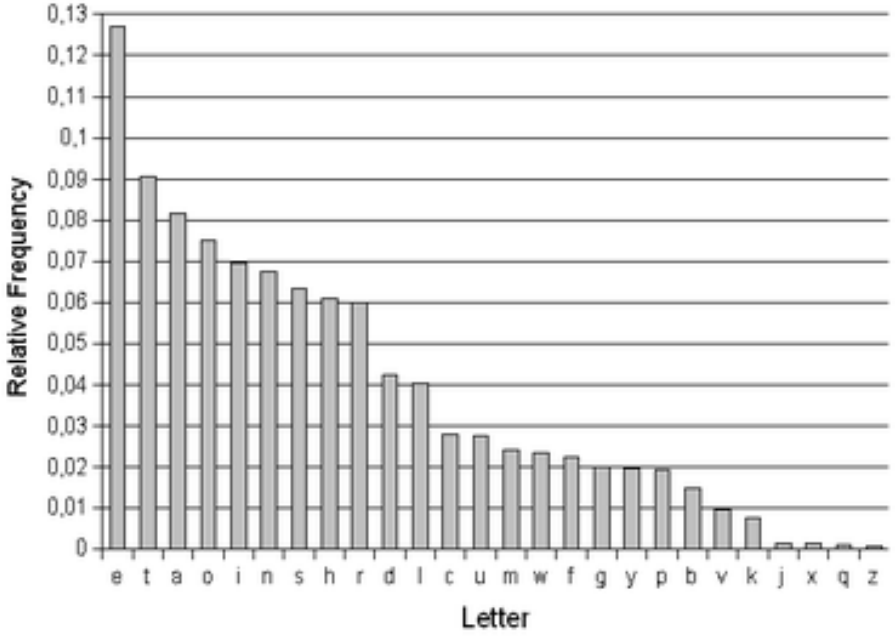
i. Implicit Assumption: K = 3

Plaintext:	A	B	C	D	E	F	…	Z
Cipher: (K = 3)	D	E	F	G	H	I	…	C

Historical Breakthrough: Exposed Weaknesses

- Critical Weakness of Caesar Cipher was discovered almost 800 years after its Invention!
- **Al-Kindi**
  - Frequency Analysis:
    - Observe the frequency of the letters that composite the ciphertext.
    - Observe the frequency of the letters that composite the language.
    - Guess the correct key/shift through trial/error
  - In the English language, the most frequently appearing characters are:
    - A, E, O, T, ...

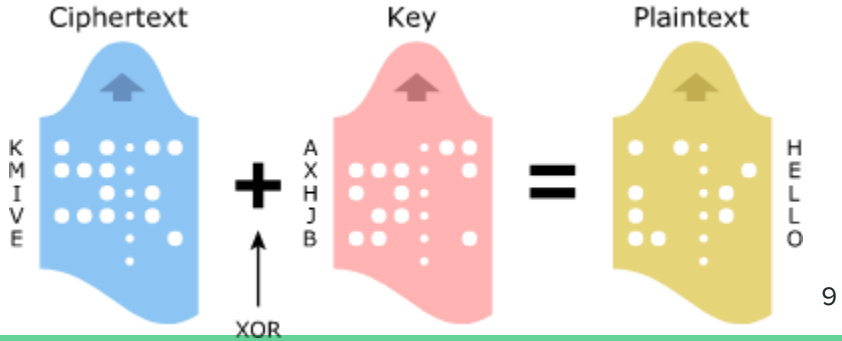
Frequency Analysis on the English Language



Historical Applications

3. **Motivations for Newer Ciphers**
    a. Vigenere
    b. Vernam System
    c. Enigma Machine

	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



Historical Applications

1. Newspaper Lovers
2. Russia versus Germany (WWI)
3. Bernardo Provenzano [Mafioso King]
4. Enigma Machine

Bernardo Provenzano

Enigma Machine

- Used by the Nazi’s to encrypt their messages

Technical Applications

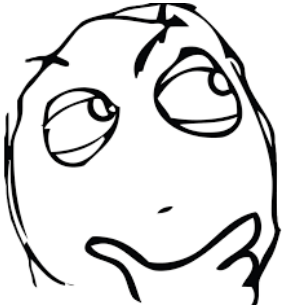
1. **ROT13 System**
   a. Used on many forums and blogs to easily, “hide” spoilers.
   b. K = 13

Plaintext:	A	B	C	D	E	F	…	Z
Cipher: (K = 13)	N	O	P	Q	R	S	…	M

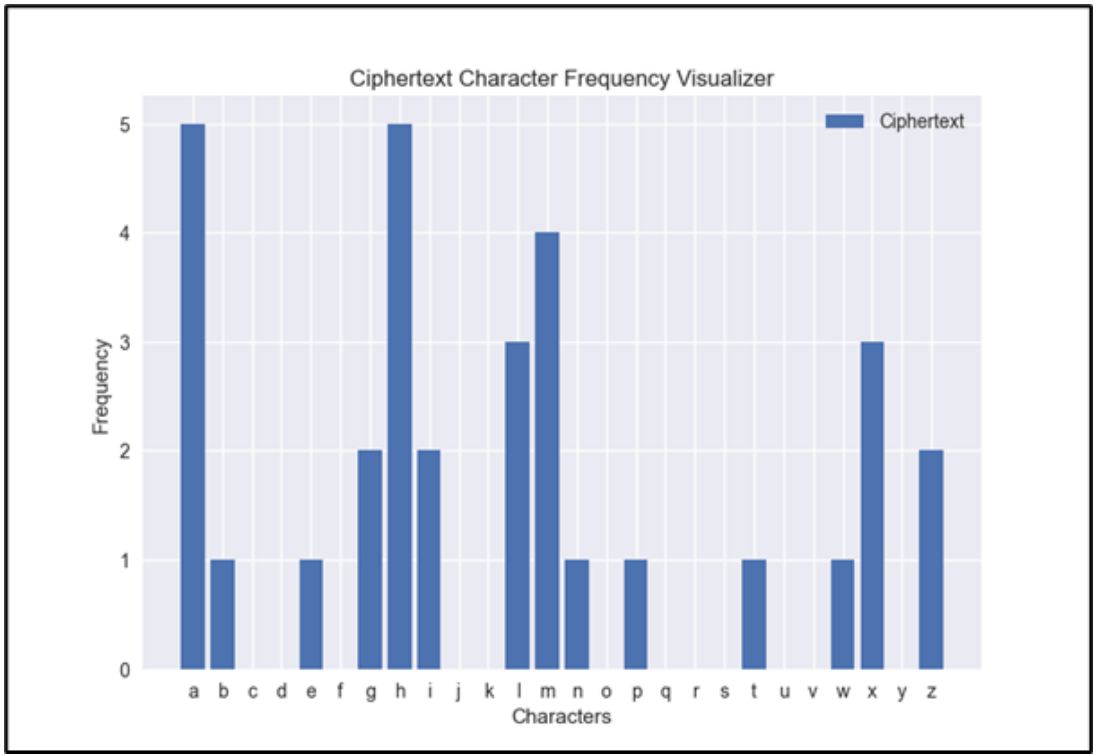
Cipher Demo

- **Intercepted Ciphertext:**
  - **“ZHHWM ABGZL ATIIX GMHMA HLXPA HANLM EX”**

- What should we do with this?
  - Al-Kindi’s Frequency Analysis Technique!!



Cipher Evaluation



- **Possible Key Candidates:**
  - A ⇒ A
  - A ⇒ E
  - A ⇒ O
  - A ⇒ T

  (...)

  - A ⇒ H
  - E ⇒ H
  - H ⇒ O
  - H ⇒ T

Cipher Evaluation

- **Possible Key Candidates:**
  - A ⇒ A ❌
    - zhhwm abgzl atiix gmhma hlxpa hanlm ex
  - A ⇒ E ❌
    - vddsi wxcvh wpeet cidiw dhtlw dwjhi at
  - A ⇒ O ❌
    - lttiy mnslx mfuuj sytym txjbm tmzxy qj
  - **A ⇒ T** ✅
    - **goodt hings happe ntoth osewh ohust le**

“Good things happen to those who hustle” - Caesar, Probably

Cipher Evaluation {Kerckhoff's Principle for Analysis}

1. The System Must Be Practically, If Not Mathematically, Indecipherable
2. It Should Not Require Secrecy, and it Should Not Be a Problem if it Falls into Enemy Hands
3. It Must Be Possible to Communicate and Remember the Key Without Using Written Notes, and Correspondents Must Be Able to Change or Modify it at Will
4. It Must Be Applicable to Telegraph Communications
5. It Must Be Portable, and Should Not Require Several Persons to Handle or Operate
6. Lastly, Given the Circumstances in Which it is to be Used, the System Must Be Easy to Use and Should Not Be Stressful to Use or Require Its User to Know and Comply With a Long List of Rules

Concluding Thoughts

References

[1] J. Holden, “Chapter 1: Introduction to Ciphers and Substitution,” in The Mathematics of Secrets: Cryptography from Caesar Ciphers to Digital Encryption, Princeton, NJ, New Jersey: Princeton University Press, 2019, pp. 1–29.

[2] D. Luciano and G. Prichett, “Cryptology: From caesar ciphers to public-key cryptosystems,” The College Mathematics Journal, vol. 18, no. 1, pp. 2–17, 1987.

[3] A. Jain, R. Dedhia, and A. Patil, “Enhancing the security of caesar cipher substitution method using a randomized approach for more secure communication,” International Journal of Computer Applications, vol. 129, no. 13, pp. 6–11, Nov. 2015.

[4] “The story of Cryptography: History,” The Story of Cryptography : Historical Cryptography. [Online]. Available: https://ghostvolt.com/articles/cryptography_history.html. [Accessed: 01-Feb-2022].

[5] Caesar cipher. [Online]. Available: https://www.cs.mcgill.ca/~rwest/wikispeedia/wpcd/wp/c/Caesar_cipher.htm. [Accessed: 01-Feb-2022].

[6] The Caesar cipher | Journey into cryptography | Computer Science | Khan Academy. YouTube, 2012.

[7] F. C. Piper and S. Murphy, “Chapter 3: Historical Algorithms, Simple Examples,” in Cryptography: A very short introduction, Oxford, Mississippi: Oxford University Press, 2002, pp. 18–32.

[8] S. Sutherland and S. R. Simanca, “Simple Ciphers,” Simple ciphers. [Online]. Available: http://www.math.stonybrook.edu/~scott/papers/Book331/Simple_Ciphers.html. [Accessed: 01-Feb-2022].

[9] “Kerckhoffs's principle,” Wikipedia, 21-Nov-2021. [Online]. Available: https://en.wikipedia.org/wiki/Kerckhoffs%27s_principle. [Accessed: 08-Feb-2022].

[10] R. F. Churchhouse, Codes and ciphers: Julius Caesar, the Enigma, and the internet. Cambridge, Massachusetts: Cambridge University Press, 2002.

[11] CrashCourse, “Cryptography: Crash course computer science #33 - YouTube,” YouTube, 25-Oct-2017. [Online]. Available: https://www.youtube.com/watch?v=jhXCTbFnK8o. [Accessed: 11-Feb-2022].

[12] “Bernardo Provenzano,” Wikipedia, 05-Feb-2022. [Online]. Available: https://en.wikipedia.org/wiki/Bernardo_Provenzano. [Accessed: 11-Feb-2022].