

Cryptanalysis 101

Breaking Caesar and Vigenère Ciphers

Tony Arcieri
@bascule



This dude and his daughter
really love frequency analysis

Cryptanalysis = Crypto Breaking

- Today's exercise is intended for complete beginners
- Computer required!
- Programming also required



Vigenère ciphers? I broke my first Playfair cipher when I was 5. At least ask me to break CBC mode using a padding oracle



COOL STORY, BRO

Caesar Cipher

You know ROT13 right?

A => N

B => O

C => P

D => Q

E => R

F => S

G => T

Caesar Cipher

ROT-N, where N is the key

Caesar cipher for N=1

A \Rightarrow B

B \Rightarrow C

C \Rightarrow D

D \Rightarrow E

E \Rightarrow F

F \Rightarrow G

G \Rightarrow H

Caesar Cipher

ROT-N, where N is the key

Caesar cipher for N=2

A \Rightarrow C

B \Rightarrow D

C \Rightarrow E

D \Rightarrow F

E \Rightarrow G

F \Rightarrow H

G \Rightarrow I

Breaking Caesar Ciphers



How does it work?

Frequency Analysis

- Write a function which computes the probability that a plaintext is English
- Brute force all of the possible decrypts
- Pick the one that has the most English-like letter frequency distribution

English Letter Frequencies

Top 10 most commonly used letters

"E" => 0.104

"T" => 0.072

"A" => 0.065

"O" => 0.059

"N" => 0.056

"I" => 0.055

"S" => 0.051

"R" => 0.049

"H" => 0.049

"D" => 0.034

COPY THIS DOWN

English Letter Frequencies

Top 10 most commonly used letters

"E" => 0.104

"T" => 0.072

"A" => 0.065

"O" => 0.059

"N" => 0.056

"I" => 0.055

"S" => 0.051

"R" => 0.049

"H" => 0.049

"D" => 0.034

Write a function: `tastes_like_english(text)`

Calculate the average letter frequency

English Letter Frequencies

Top 10 most commonly used letters

"E" => 0.104

"T" => 0.072

"A" => 0.065

"O" => 0.059

"N" => 0.056

"I" => 0.055

"S" => 0.051

"R" => 0.049

"H" => 0.049

"D" => 0.034

`tastes_like_english("english") == 0.045`

Write a Caesar Cipher Solver

SZAP QFWW JESP CPLC
PXZC PESL YAPZ AWPB
SZHT WWDZ WGPE STD

- Write a rotN decryption function
- Brute force all possible decrypts
- Pick the one with the highest letter frequency

Solution

DONTTELLMETHATYOU DIDN'T HEAR DEF CON WAS CANCELLED

ROT14

Vigenère Cipher

Multiple Caesar Ciphers keyed with a secret word

Vigenère Cipher

Multiple Caesar Ciphers keyed with a secret word

“ABC”

Vigenère Cipher

Multiple Caesar Ciphers keyed with a secret word

“ABC”

Letter 1	Letter 2	Letter 3	Letter 4
A => A	A => B	A => C	A => A
B => B	B => C	B => D	B => B
C => C	C => D	C => E	C => C
D => D	D => E	D => F	D => D
E => E	E => F	E => G	E => E
F => F	F => G	F => H	F => F
G => G	G => H	G => I	G => G

Breaking Vigenère Ciphers

- Vigenère ciphers are made out of multiple Caesar ciphers
- We already wrote a Caesar cipher solver (right?)
- Break Vigenère ciphertext apart and try to solve it as multiple Caesar ciphers

X N D F J R B

X	F	B
---	---	---

N	J
---	---

D	R
---	---

Break Vigenère Cipher

Win a merit badge!

MYYV QMJW GXNU CFSV VLNI YCAY
JCVV VYHQ ZVZR MYCR SQLA MUVF
ISMK QFTK YTXI RAXT TNYM PCGP
KZNI ESDM VHUY XAGI IVDK BMEG
ZXAX ICRE XVIW HWDY EXGI LMZH
KUXZ VMHR QINT ROXP ICXU RXKH
WVQM XPXM MRFO XTID MKBK VEPK
VVHV FXIZ SSIW ZV