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



Caesar Cipher You know ROT13 right?

 $\begin{array}{rcrcr} A & \Longrightarrow & N \\ B & \Longrightarrow & O \\ C & \Longrightarrow & P \\ D & \Longrightarrow & Q \\ E & \Longrightarrow & Q \\ E & \Longrightarrow & R \\ F & \Longrightarrow & S \\ G & \Longrightarrow & T \end{array}$

Caesar Cipher

ROT-N, where N is the key

Caesar cipher for N=1

 $\begin{array}{rcl} A & \Longrightarrow & B \\ B & \Longrightarrow & C \\ C & \Longrightarrow & D \\ D & \Longrightarrow & D \\ D & \Longrightarrow & F \\ F & \Longrightarrow & F \\ F & \Longrightarrow & G \\ G & \Longrightarrow & H \end{array}$

Caesar Cipher

ROT-N, where N is the key

Caesar cipher for N=2

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
"0" => 0.059
"N" => 0.056
"I" => 0.055
"S" => 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
"0" => 0.059
"N" => 0.056
"I" => 0.055
"S" => 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
"0" => 0.059
"N" => 0.056
"I" => 0.055
"S" => 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

SZAPQFWWJESPCPLCPXZCPESLYAPZAWPHSZHTWWDZWGPESTD

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

Solution

DONTTELLMETHATYOUDIDNTHEARDEFCONWASCANCELLED

ROT14

Vigenère Cipher

Multiple Caesar Ciphers keyed with a secret word

Vigenère Cipher Multiple Caesar Ciphers keyed with a secret word "ABC"

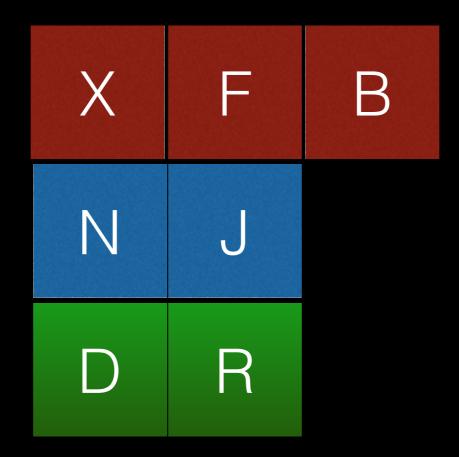
Vigenère Cipher Multiple Caesar Ciphers keyed with a secret word "ABC"

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

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





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