An Introductory Cryptology Class for Both Math and Non-Math Majors

Jennifer Bready, PhD
Mount Saint Mary College
Newburgh, NY

45th Annual AMATYC Conference
November 17, 2019

“There’s no money in the budget for data encryption, so I just rearranged all the letters on your keyboard.”
Frequency Analysis

Relative Letter Frequency

- A: 12%
- B: 8%
- C: 6%
- D: 4%
- E: 14%
- F: 2%
- G: 4%
- H: 6%
- I: 2%
- J: 2%
- K: 2%
- L: 2%
- M: 2%
- N: 4%
- O: 6%
- P: 2%
- Q: 2%
- R: 4%
- S: 8%
- T: 4%
- U: 2%
- V: 2%
- W: 2%
- X: 2%
- Y: 2%
- Z: 2%
# Frequency Analysis

<table>
<thead>
<tr>
<th>digraph</th>
<th>relative freq. (%)</th>
<th>digraph</th>
<th>relative freq. (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>TH</td>
<td>3.319</td>
<td>ES</td>
<td>1.213</td>
</tr>
<tr>
<td>HE</td>
<td>2.859</td>
<td>TO</td>
<td>1.213</td>
</tr>
<tr>
<td>IN</td>
<td>2.081</td>
<td>NT</td>
<td>1.200</td>
</tr>
<tr>
<td>ER</td>
<td>1.596</td>
<td>EA</td>
<td>1.059</td>
</tr>
<tr>
<td>ED</td>
<td>1.493</td>
<td>OU</td>
<td>1.047</td>
</tr>
<tr>
<td>AN</td>
<td>1.430</td>
<td>NG</td>
<td>1.034</td>
</tr>
<tr>
<td>ND</td>
<td>1.430</td>
<td>ST</td>
<td>1.034</td>
</tr>
<tr>
<td>AR</td>
<td>1.302</td>
<td>AS</td>
<td>0.996</td>
</tr>
<tr>
<td>RE</td>
<td>1.302</td>
<td>RO</td>
<td>0.996</td>
</tr>
<tr>
<td>EN</td>
<td>1.289</td>
<td>AT</td>
<td>0.983</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>trigraph</th>
<th>relative freq. (%)</th>
<th>trigraph</th>
<th>relative freq. (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>THE</td>
<td>1.82</td>
<td>EAR</td>
<td>0.26</td>
</tr>
<tr>
<td>AND</td>
<td>0.77</td>
<td>HAT</td>
<td>0.24</td>
</tr>
<tr>
<td>ING</td>
<td>0.68</td>
<td>OFT</td>
<td>0.22</td>
</tr>
<tr>
<td>HER</td>
<td>0.50</td>
<td>WAS</td>
<td>0.21</td>
</tr>
<tr>
<td>NTH</td>
<td>0.40</td>
<td>EST</td>
<td>0.21</td>
</tr>
<tr>
<td>ENT</td>
<td>0.36</td>
<td>HEN</td>
<td>0.20</td>
</tr>
<tr>
<td>THA</td>
<td>0.35</td>
<td>IVE</td>
<td>0.20</td>
</tr>
<tr>
<td>INT</td>
<td>0.30</td>
<td>ALL</td>
<td>0.20</td>
</tr>
<tr>
<td>ERE</td>
<td>0.29</td>
<td>THI</td>
<td>0.20</td>
</tr>
<tr>
<td>DTH</td>
<td>0.28</td>
<td>HIN</td>
<td>0.20</td>
</tr>
</tbody>
</table>
Why Cryptology?

• Accessible to anyone
• Covers multiple mathematics topics
• Interesting history
• Applicable to many majors
Math Topics Covered

• Number Theory: primes, relatively prime, modular arithmetic and congruences, inverses, Fermat’s Little Theorem, the Euclidean Algorithm, Euler’s phi function

• Linear Algebra: matrix multiplication, determinants, inverses

• Basic probability and statistics
  – Frequency analysis
Cryptology is the study of secret writing, or codes. While many students know that when they purchase items online their information must be encrypted, they may not realize the mathematics used to keep their information safe. Cryptology covers diverse areas of mathematics which include number theory, linear algebra, probability, and statistics. This course will be a study of both classic and modern secret writing, specifically looking at the mathematics involved with each cipher and how to ‘attack’ them, i.e. students will learn both enciphering and deciphering techniques.
Topic Overview

• Weeks 1-3: Polybius Squares, Caesar, shift, and affine ciphers, congruences, frequency analysis, Sukhotin’s method; Test 1

• Weeks 4-6: Vigenere cipher, Index of Coincidence and Kasiski method, transposition ciphers; Test 2
Topic Overview

• Weeks 7-9: Wheel ciphers, Pigpen and Sir Francis Bacon, Playfair cipher, ADFGV and ADFGVX, 2x2 Hill Cipher; Test 3

• Weeks 10-12: 3x3 Hill Cipher, Fermat’s Little Theorem, Euclidean Algorithm, public-key cryptography and RSA; Test 4
Final Presentation

• Group presentations on a topic NOT covered in class. Previous topics include:
  – Zodiac Killer
  – Sherlock Homes and Poe
  – Kryptos statue
  – Diffie-Hellman
  – Hash Functions
  – Bitcoin
  – Steganography
Polybius Square

- Early Greek cryptography, but used later with the ADFGX cipher during WWI
- Encipher: MATH

Polybius square was also used as a “Knock” cipher for captured POW’s in Vietnam
Caesar and Shift Ciphers

- First introduction to congruences
- Caesar cipher is a shift of 3, but can add any number: $C_i \equiv P_i + 3 \pmod{26}$
- To decipher: $P_i \equiv C_i - 3 \pmod{26}$
Caesar and Shift Ciphers

• AMATYC = DPDWBF
  A: $C \equiv 0 + 3 \equiv 3 \pmod{26}$
  M: $C \equiv 12 + 3 \equiv 15 \pmod{26}$
  T: $C \equiv 19 + 3 \equiv 22 \pmod{26}$
  Y: $C \equiv 24 + 3 \equiv 27 \equiv 1 \pmod{26}$
  C: $C \equiv 2 + 3 \equiv 5 \pmod{26}$

• BHWL = ???
  B: $P \equiv 1 - 3 \equiv -2 \equiv 24 \pmod{26} \rightarrow Y$
  H: $P \equiv 7 - 3 \equiv 4 \pmod{26} \rightarrow E$
  W: $P \equiv 22 - 3 \equiv 19 \pmod{26} \rightarrow T$
  L: $P \equiv 11 - 3 \equiv 8 \pmod{26} \rightarrow I$
Affine Ciphers

- **To encipher:**  \( C \equiv aP + b \pmod{26} \)
  - Note: \( a \) must be relatively prime to 26 in order to decipher.
  - Which integers satisfy \((a, 26)=1\)?
    - 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25

- **Euler’s phi function:**  \( \phi(26) = 12 \)
  - The number of integers relatively prime to a number
Affine Ciphers

• To decipher: \( P \equiv \bar{a} (C - b) \pmod{26} \)
  is the inverse of \( a \)

• Finding inverses
  – Given an integer \( a \) with \((a, m)=1\), a solution is called an inverse of \( a \) if it satisfies:
    \[ ax \equiv 1 \pmod{26} \]

• The inverses of \((a, 26)=1\): \( \bar{3} = 9, \bar{5} = 21, \bar{7} = 15, \ldots \)
  – 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25
Vigenere Cipher

- Polyalphabetic cipher
- Uses a keyword to encrypt: \( P_i \equiv C_i + K_i \pmod{26} \)

Plain text:

<table>
<thead>
<tr>
<th>M</th>
<th>I</th>
<th>L</th>
<th>W</th>
<th>A</th>
<th>U</th>
<th>K</th>
<th>E</th>
<th>E</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>8</td>
<td>11</td>
<td>22</td>
<td>0</td>
<td>20</td>
<td>10</td>
<td>4</td>
<td>4</td>
</tr>
</tbody>
</table>

Keyword:

<table>
<thead>
<tr>
<th>F</th>
<th>O</th>
<th>N</th>
<th>Z</th>
<th>F</th>
<th>O</th>
<th>N</th>
<th>Z</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>14</td>
<td>13</td>
<td>25</td>
<td>5</td>
<td>14</td>
<td>13</td>
<td>25</td>
<td>5</td>
</tr>
</tbody>
</table>

Convert to modulus 26:

| 17| 22| 24| 21| 5 | 8 | 23| 3 | 9 |

Cipher text:

| R | W | Y | V | F | I | X | D | J |

Both “E’s” enciphered as different letters
Vigenere Decipher

- Index of Coincidence (IC) – used to find the length of the keyword
  \[
  IC = \sum \frac{(f_i \times (f_i - 1))}{n(n-1)} \quad k \approx \frac{0.0265n}{(0.065 - I) + n(I - 0.0385)}
  \]
- Kasiski test – find repeated strings and count the distances. The GCD of the distances is often the keyword length.
Vigenere Cipher Project

• Students use technology to encrypt a 400-500 word passage with a keyword of length between 3 and 6.
• Messages are randomly passed to another group.
• Students calculate the IC, keyword length, and Kasiski to predict the length of the keyword.
• Frequency analysis is used to find the keyword and decrypt.
Transposition Ciphers

• Rail fence cipher
  – Encipher: PLAN THE ATTACK with key of 3
  – Cipher text: PTTKLNHATCAEA

```
  P  T  T  K
  L  N  H  A  T  C
  A  E  A
```

Transposition Ciphers

• Columnar cipher

Enchiper: HOW CAN WE MAKE THIS MORE TRICKY with keyword MATH

– Fill in the sentence going across the rows
– Add keyword and encipher in alphabetical order

<table>
<thead>
<tr>
<th>M</th>
<th>A</th>
<th>T</th>
<th>H</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>1</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>H</td>
<td>O</td>
<td>W</td>
<td>C</td>
</tr>
<tr>
<td>A</td>
<td>N</td>
<td>W</td>
<td>E</td>
</tr>
<tr>
<td>M</td>
<td>A</td>
<td>K</td>
<td>E</td>
</tr>
<tr>
<td>T</td>
<td>H</td>
<td>I</td>
<td>S</td>
</tr>
<tr>
<td>M</td>
<td>O</td>
<td>R</td>
<td>E</td>
</tr>
<tr>
<td>T</td>
<td>R</td>
<td>I</td>
<td>C</td>
</tr>
<tr>
<td>K</td>
<td>Y</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

Cipher text: ONAHORY CEESECX HAMTMTK WWKIRIX

Send: ONAHO RYCEE SECXH AMTMTMT KWWKI RIX
Playfair Cipher

• Uses a 5x5 square and a keyword.
• Break letters into two; insert an X for repeated letters:
• Rules:
  – Same column shift down
  – Same row shift right
  – Forms a box, swap opposite corners
Playfair Cipher

- Encipher ADDITION with keyword YOUTH
- AD XD IT IO NX = BE TK KU GU QV
ADFGX / ADFGVX

- Uses both a Polybius square and columnar transposition
- ADFGX was used because the letters were very distinct in Morse code
- ADFGX creates a 5x5 square, whereas ADFGVX creates a 6x6 square (can add 0 – 9)
ADFGX Example

- Encipher the word JOKER using the matrix keyword BATMAN and the columnar keyword BANE

<table>
<thead>
<tr>
<th>A</th>
<th>D</th>
<th>F</th>
<th>G</th>
<th>X</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>B</td>
<td>A</td>
<td>T</td>
<td>M</td>
</tr>
<tr>
<td>D</td>
<td>C</td>
<td>D</td>
<td>E</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>H</td>
<td>I/J</td>
<td>K</td>
<td>L</td>
</tr>
<tr>
<td>G</td>
<td>P</td>
<td>Q</td>
<td>R</td>
<td>S</td>
</tr>
<tr>
<td>X</td>
<td>V</td>
<td>W</td>
<td>X</td>
<td>Y</td>
</tr>
</tbody>
</table>

JOKER = FD FX FF DF GF XF

<table>
<thead>
<tr>
<th>B</th>
<th>A</th>
<th>N</th>
<th>E</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>1</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>F</td>
<td>D</td>
<td>F</td>
<td>X</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>D</td>
<td>F</td>
</tr>
<tr>
<td>G</td>
<td>F</td>
<td>X</td>
<td>F</td>
</tr>
</tbody>
</table>

= DFF FFG XFF FDX
Hill Cipher

• Lester Hill, 1929
• Uses matrices, 2x2 or 3x3
• Determinants must be relatively prime to 26 in order to find inverses. Encipher: TRY

\[
\begin{pmatrix}
2 & 1 & 4 \\
3 & 5 & 2 \\
1 & 1 & 1 \\
\end{pmatrix}
\begin{pmatrix}
19 \\
17 \\
24 \\
\end{pmatrix}
= 
\begin{pmatrix}
151 \\
190 \\
108 \\
\end{pmatrix}
\equiv 
\begin{pmatrix}
21 \\
8 \\
4 \\
\end{pmatrix}
\mod 26
\]

T = 19  \Rightarrow  21 = V
R = 17  \Rightarrow  8 = I
Y = 24  \Rightarrow  4 = E
Hill Cipher Project

• Students create a matrix that meets the requirements for a Hill matrix.
• Encipher a 20-30 word sentence.
• Pass encipher matrix and encrypted sentence.
• Students find the decipher matrix and try to decrypt the message
  – Many steps involved to find the decipher matrix, involving determinants and inverse matrices.
• Movie night!
  – Watch The Imitation Game, and discuss fact vs. fiction
  – Video on how the Enigma works
Public Key / RSA

- Students learn the Euclidean algorithm to find greatest common divisors and inverses
- Fermat’s Little theorem: \( a^{p-1} \equiv 1 \pmod{p} \)
- Repeated squaring
- Formula’s for Euler’s phi-function
  \[ \phi(p^a) = p^a - p^{a-1} \]
Alice and Bob want to share a message

Eve wants to eavesdrop
  - Alice uses Bob’s public key to encrypt a private message
  - Bob uses his private key to decrypt the message
  - Alice decrypts Bob’s message with her private key
  - Eve can’t read any of it!
Public Key / RSA

- Select two large primes, $p$ and $q$.
  \[ n = pq \quad \text{and} \quad \phi(n) = (p - 1)(q - 1) \]
- Choose an encryption key $e$ such that \((e, \phi(n)) = 1\)
- Calculate $d$ the decryption key with the property \(ed \equiv 1(\phi(n))\)

Public key: \(n\) and \(e\)  
Private key: \(d\)
Public Key / RSA

• To encrypt:
  – Must be able to simplify large exponents mod $n$
    \[ c \equiv m^e \pmod{n} \]

• To decrypt:
  – Must be able to calculate $d$, but can use the Euclidean algorithm to find the inverse
    \[ m \equiv c^d \pmod{n} \]
RSA Example

• Let p=11, q=3
  – Then n = 11x3=33, and phi(n)=(11-1)(3-1)=20
  – Select an e that is relatively prime to 20.
    \[ c \equiv m^3 \pmod{33} \]
  – Encrypt H = 7
    \[ c \equiv 7^3 \pmod{33} \]
    \[ 13 \equiv 343 \pmod{33} \]
RSA Example

- To decrypt, need the inverse of $3 \pmod{20}$
  - Use the Euclidean Algorithm
  - To decrypt, use
    - $m \equiv c^7 \pmod{33}$
  - Use the method of repeated squaring to reduce

\[
\begin{align*}
20 &= 6(3) + 2 & 1 &= 3 - 1(2) \\
3 &= 1(2) + 1 & 1 &= 3 - 1[20 - 6(3)] \\
2 &= 2(1) + 0 & 1 &= 7(3) - 1(20) \\
\end{align*}
\]
\[
\begin{align*}
m &= 13^7 \pmod{33} \\
m &= (13^2)(13^2)(13^2)(13) \pmod{33} \\
m &= (4)(4)(4)(13) \pmod{33} \\
m &= (-2)(13) \pmod{33} = -26 = 7 \pmod{33}
\end{align*}
\]
Questions?

Contact Info:

Jennifer Bready
jen.bready@msmc.edu
845-569-3268

Sir Francis Bacon cipher

KNOWLEDGE IS POWER