Unit 9: Cryptography

Dave Abel

April 11th, 2016
Python Workshops

› Monday at 6pm-8pm in Lubrano (4th floor CIT)

› Tuesday at 7pm-9pm in Lubrano (4th floor CIT)

› Project Proposal Form due Friday (must be completed if you want to do the python project)
  - Choose Game, Machine Learning, Visualization, or coordinate something else with me.
Recursion Reading

The Recursive Mind
The Origins of Human Language, Thought, and Civilization

Michael C. Corballis
Cryptography: Takeaway

We can use computation to simulate a lock and key!
Cryptography: Takeaway

We can use computation to simulate a lock and key!

We can be confident in the security of our digital systems
Outline

‣ Alice, Bob, and Eve

‣ Classical Cryptography (2000 B.C.E. -1900 A.D.)
  - Ciphers
  - Breaking Classical Cryptographic Systems

‣ Modern Cryptography (1900 A.D. - today!)
  - One Way Functions
  - Public Key Cryptography + Diffie-Helman
  - Randomness!

‣ Political and Legal relevance
Alice, Bob, Eve
Alice, Bob, Eve
Alice, Bob, Eve
Alice, Bob, Eve
Q: If Alice and Bob know Eve may eavesdrop, how can Alice send the message so Bob can still read it?
Alice, Bob, Eve
Alice, Bob, Eve
Problem Specification: Secure Communication

- INPUT: A plaintext message that Alice wants to send to Bob.

- OUTPUT: An encrypted message, such that Bob can extract the original plaintext, but Eve cannot.
Problem Specification: Secure Communication

- INPUT: A *plaintext* message that Alice wants to send to Bob.

- OUTPUT: An *encrypted* message, such that Bob *can* extract the original *plaintext*, but Eve cannot.

The central goal of Cryptography is solving this problem.
Some Terminology

• **Definition:** a message is *plaintext* if it is not encrypted or obscured in any way.

• **Definition:** a message is *encrypted* if it can only be (easily) read by authorized readers.

• **Definition:** turning a plaintext message into an encrypted message is the process of *encryption*.

• **Definition:** turning an encrypted message into a plaintext message is the process of *decryption*. 
Some History

- Cryptography comes from the Greek, Krypto, meaning “hidden”, and graphein, meaning “writing”.

- Earliest known use of encryption is in Egyptian Hieroglyphs, dating back to 1900 B.C.E.

- Also used in Ancient Greece, Rome, and Mesopotamia. Primarily for military use!
Some History: Greeks

- Alice and Bob each have the same funny shaped object (called a “scytale”)

- Alice writes her message around the object, sends the message to Bob.

- Bob receives the message and wraps it around the object.
Some History: Greeks
Some History: Romans

- Julius Caesar (100 B.C.E. - 40 B.C.E.) had his army communicate using encryption.

- Here’s how it worked:
  - Pick a number between 1 and 25
  - Shift each character in your message by that many characters in the alphabet.

- Called the Caesar Cipher

http://www.secretcodebreaker.com/history2.html
Caesar Cipher

- Suppose we want to encrypt “Hello”

   - Pick a number between 1 and 25
   - Shift each character in your message by that many characters in the alphabet.
Caesar Cipher

- Suppose we want to encrypt “Hello”

Caesar Cipher

- Pick a number between 1 and 25
- Shift each character in your message by that many characters in the alphabet.
Caesar Cipher

- Suppose we want to encrypt “Hello”
- Let’s choose: 4

Pick a number between 1 and 25
- Shift each character in your message by that many characters in the alphabet.
Caesar Cipher

- Suppose we want to encrypt “Hello”
- Let’s choose: 4

- Pick a number between 1 and 25
- Shift each character in your message by that many characters in the alphabet.
Caesar Cipher

- Suppose we want to encrypt “Hello”
- Let’s choose: 4
- “H” : ..., H, I, J, K, L, M

- Pick a number between 1 and 25
- Shift each character in your message by that many characters in the alphabet.

Caesar Cipher
Caesar Cipher

- Suppose we want to encrypt “Hello”
- Let’s choose: 4
- “H” : …, H, I, J, K, L, M

encrypted: \text{L}

- Pick a number between 1 and 25
- Shift each character in your message by that many characters in the alphabet.
Caesar Cipher

› Suppose we want to encrypt “Hello”

› Let’s choose: 4

› “e” : ... e, f, g, h, i, j

encrypted: L

- Pick a number between 1 and 25
- Shift each character in your message by that many characters in the alphabet.

Caesar Cipher
Caesar Cipher

• Suppose we want to encrypt “Hello”

• Let’s choose: 4

• “e” : … e, f, g, h, i, j

encrypted: L

- Pick a number between 1 and 25
- Shift each character in your message by that many characters in the alphabet.
Caesar Cipher

- Suppose we want to encrypt “Hello”
- Let’s choose: 4
- “e” : … e, f, g, h, i, j

encrypted: Li
Caesar Cipher

- Suppose we want to encrypt “Hello”
- Let’s choose: 4
- “l” : ...l, m, n, o, p

Caesar Cipher encrypted: **Li**

- Pick a number between 1 and 25
- Shift each character in your message by that many characters in the alphabet.
Suppose we want to encrypt “Hello”

Let’s choose: 4

“l” : …l, m, n, o, p

encrypted: Li

Pick a number between 1 and 25

Shift each character in your message by that many characters in the alphabet.
Caesar Cipher

- Suppose we want to encrypt “Hello”
- Let’s choose: 4
- “l”: ...l, m, n, o, p

encrypted: **Lipp**

- Pick a number between 1 and 25
- Shift each character in your message by that many characters in the alphabet.

*Caesar Cipher*
Caesar Cipher

‣ Suppose we want to encrypt “Hello”

‣ Let’s choose: 4

‣ “o” : …o, p, q, r, s

encrypted: Lipp

- Pick a number between 1 and 25
- Shift each character in your message by that many characters in the alphabet.
Suppose we want to encrypt “Hello”

- Let’s choose: 4

“o” : …o, p, q, r, s

encrypted: Lipp

- Pick a number between 1 and 25
- Shift each character in your message by that many characters in the alphabet.
Caesar Cipher

- Suppose we want to encrypt “Hello”
- Let’s choose: 4
- “o” : …o, p, q, r, s

encrypted: Lipps

- Pick a number between 1 and 25
- Shift each character in your message by that many characters in the alphabet.

Caesar Cipher
Caesar Cipher: Decryption

• Suppose we want to decrypt “Lipps”

• We chose: 4

  decrypted:

  Given the chosen number between 1 an 25…

  Shift each character in your message **back** by that many characters in the alphabet.

  Caesar Cipher: Decryption
Caesar Cipher: Decryption

- Suppose we want to decrypt “Lipps”
- We chose: 4

- Given the chosen number between 1 an 25…
- Shift each character in your message **back** by that many characters in the alphabet.

Caesar Cipher: Decryption
Caesar Cipher: Decryption

- Suppose we want to *decrypt* “Lipps”

- We chose: 4


  - Given the chosen number between 1 and 25…
  
  - Shift each character in your message **back** by that many characters in the alphabet.

  decrypted:
Caesar Cipher: Decryption

- Suppose we want to decrypt “Lipps”
- We chose: 4

**decrypted:** H

- Given the chosen number between 1 and 25…
- Shift each character in your message **back** by that many characters in the alphabet.
Caesar Cipher: Decryption

- Suppose we want to decrypt “Lipps”
- We chose: 4
- “i” : … d, e, f, g, h, i, …

decrypted: H

Given the chosen number between 1 an 25…

Shift each character in your message **back** by that many characters in the alphabet.
Caesar Cipher: Decryption

› Suppose we want to decrypt “Lipps”

› We chose: 4

› “i” : … d, e, f, g, h, i, …

- Given the chosen number between 1 an 25…

- Shift each character in your message **back** by that many characters in the alphabet.

decrypted: H
Caesar Cipher: Decryption

› Suppose we want to decrypt “Lipps”

› We chose: 4

› “i” : … d, e, f, g, h, i, …

decrypted: He

- Given the chosen number between 1 and 25…
- Shift each character in your message **back** by that many characters in the alphabet.
Caesar Cipher: Decryption

- Suppose we want to decrypt “Lipps”
- We chose: 4
- “p” : ... l, m, n, o, p, ...

  **back**

- Given the chosen number between 1 an 25...
- Shift each character in your message **back** by that many characters in the alphabet.

  decrypted: **Hello**
Caesar Cipher
Caesar Cipher

‣ One point: going off the end of the alphabet is like the $mod$ operator!

‣ Suppose we shift “xyz” by 4:

‣ “x” : …x, y, z, a, b, c…

‣ “y” : …y, z, a, b, c, d…

‣ “z” : …z, a, b, c, d, e…
Caesar Cipher

› One point: going off the end of the alphabet is like the mod operator!

› Suppose we shift “xyz” by 4:

› “x” : …x, y, z, a, b, c…

› “y” : …y, z, a, b, c, d…

› “z” : …z, a, b, c, d, e…
Caesar Cipher

- One more point: all non-character symbols stay the same.

- Suppose we shift “Howdy! I’m Dave.” by 2:

- We get: Jqyfa! K’o Fcxg.
Q: With a shift value of 2, what is the Caesar encryption of: “Where there is love”
Clicker Question!

Q: With a shift value of 2, what is the Caesar encryption of: “Where there is love”

[A] Yjdtd vjdtd lv mpwf  [C] Yjdtd wjdtd ku mpwf

[B] Yjdtd vjdtd ku nqxg  [D] Yjdtd wjdtd lv mpwf
Q: With a shift value of 2, what is the Caesar encryption of: “Where there is love”

[A] Yjdtd vjdtd lv mpwf       [C] Yjdtd wjdtd ku mpwf

[B] Yjdtd vjdtd ku nqxg       [D] Yjdtd wjdtd lv mpwf
Q: With a shift value of 2, what is the Caesar encryption of: “Where there is love”
Caesar Cipher

For this to work, *Alice* and *Bob* must meet before hand to agree on a shift amount!
One Alice and Bob agree on a shift, they can send and receive messages indefinitely! (don’t need to meet up again)

This means they’ll keep using the same shift over and over again.

Problematic.
Caesar Cipher

Encrypted message:

Jg'f hqtiqvvgp cnn cdqtwv vjg rgqrng kp enqcmu wpvkn jg rcuugf c itqwr qh vjgo pgzv vq vjg dcmgt'u. Jg gagf vjgo cpitkna cu jg rcuugf. Jg fkfp'v mpqy yja, dwv vjga ocfg jko wpgcua. Vjku dwpej ygtg yjkurgtkpi gzekvgfna, vqq, cpf jg eqwnfp'v ugg c ukping eqnngevkpi vkp. Kv ycu qp jku yca dcem rcuv vjgo, enwvejkpi c nctig fqwijpwwv kp c dci, vjcv jg ecwijv c hgy yqtfu qh yjcv vjga ygtg ucakpi.
Caesar Cipher

Encrypted message:

Jg'f hqiqvvgp cnn cdqvw vjg rgqrng kp enqcmu wpvkn jg rcuugf c itqwr qh vjgo pgzv vq vjg dcmgt'u. Jg gagf vjgo cpitkna cu jg rcuugf. Jg fkp'v mpqy yja, dwv vjga ocfg jko wpgcua. Vjku dwpej ygtg yjkurgtkpi gzekvgfna, vqq, cpf jg eqwnfp'v ugg c ukping eqnngevkpi vkp. Kv ycu qp jku yca dcem rcuv vjgo, enwvejkpi c nctig fqwijpwwv kp c dci, vjcv jg ecwijv c hgy yqtfu qh yjcv vjga ygtg uca kpi.

Q: Can we guess any letters in here?
Caesar Cipher

Encrypted message:

Jg'f hqtiqvvgp cnn cdqwv vjg rgqrng kp enqcmu wpvkn jg rcuugf c itqwr qh vjgo pgzv vq vjg dcmgt'u. Jg gagf vjgo cpitkna cu jg rcuugf. Jg fkfp'v mpqy yja, dwv vjga ocfg jko wpgcua. Vjku dwpej ygtg yjkurgtkpi gzekvgfna, vqq, cpf jg eqwnfp'v ugg c ukping eqnngevkpi vkp. Kv ycu qp jku yca dcem rcuv vjgo, enwvejkpi c nctig fqwijpwv kp c dci, vjcv jg ecwijv c hgy yqtfu qh yjcv vjga ygtg ucakpi.

Q: Can we guess any letters in here?

Q: How many one letter words are there?
Caesar Cipher

Jg'f hqtiqvvgp cnn cdqvw vjg rgqrng kp enqcmu wpvkn jg rcuugf c itqwr qh vjgo pgzv vq vjg dcmsgt'u. Jg gagf vjgo cpitkna cu jg rcuugf.

Jg fkfp'v mpqy yja, dwv vjga ocfg jko wpgcua. Vjku dwpej ygtg yjkurgtkpi gzekvgfna, vqq, cpf jg eqwnfp'v ugg c ukping eqnngevkpi vkp. Kv ycu qp jku yca dcem rcuv vjgo, enwvejkpi c nctig fqwiwpwv kp c dci, vjcv jg ecwijv c hgy yqtfu qh yjcv vjga ygtg ucakpi.

Q: How many one letter words are there?

**c** -> a, shift is 2

**c** -> i, shift is 20
Caesar Cipher

Pm'l nwzowbbmv itt ijwcb bpm xmwxtm qv ktwisa cvbqt pm xiaaml i ozwcx wn bpmu vmfb bw bpm jismz'a. Pm mgml bpmu ivozqtg ia pm xiaaml. Pm lqlv'b svwe epg, jcb bpmg uilm pqu cvmiag. Bpqa jcvkp emzm epqaxmzqvo mfkqbmltg, bww, ivl pm kwctlv'b amm i aqvotm kwttmkbqvo bqv. Qb eia wv pqa eig jiks xiab bpmu, ktcbkpqvo i tizom lwcopvcb qv i jio, bpib pm kicopb i nme ewzla wn epib bpmg emzm aigqvo.

Q: How many one letter words are there?

- c -> a, shift is 2
- c -> i, shift is 20
Caesar Cipher

He'd forgotten all about the people in cloaks until he passed a group of them next to the baker's. He eyed them angrily as he passed. He didn't know why, but they made him uneasy. This bunch were whispering excitedly, too, and he couldn't see a single collecting tin. It was on his way back past them, clutching a large doughnut in a bag, that he caught a few words of what they were saying.

Q: How many one letter words are there?

c -> a, shift is 2
c -> i, shift is 20
Caesar Cipher

He'd forgotten all about the people in cloaks until he passed a group of them next to the baker's. He eyed them angrily as he passed. He didn't know why, but they made him uneasy. This bunch were whispering excitedly, too, and he couldn't see a single collecting tin. It was on his way back past them, clutching a large doughnut in a bag, that he caught a few words of what they were saying.

Q: How many one letter words are there?

Q: How many one letter words are there?

\[c \rightarrow a, \text{shift is 2}\]

\[c \rightarrow i, \text{shift is 20}\]
Caesar Cipher

- Idea: Alice and Bob exchange a shift value. Encrypt by moving the characters forward by that value. Decrypt by moving the characters back by that value.

- Actually used by the Roman Empire!

- **Problem:** we can crack it pretty easily if we get enough text (if there’s ever a one letter word…)
Substitution Cipher

- Idea: similar to Caesar! Instead of shifting every letter the same amount, pick a fixed letter to change each letter to:
Substitution Cipher

- Idea: similar to Caesar! Instead of shifting every letter the same amount, pick a fixed letter to change each letter to:

| 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 |
| m | q | z | v | p | j | w | r | s | i | o | k | g | b | a | x | n | l | f | c | e | t | y | h | u | d |
Substitution Cipher

- Idea: similar to Caesar! Instead of shifting every letter the same amount, pick a fixed letter to change each letter to:

| 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 |
| m | q | z | v | p | j | w | r | s | i | o | k | g | b | a | x | n | l | f | c | e | t | y | h | u | d |

Example: “Hello”
Substitution Cipher

› Idea: similar to Caesar! Instead of shifting every letter the same amount, pick a fixed letter to change each letter to:

Example: “Hello”

Encrypted:
Substitution Cipher

- Idea: similar to Caesar! Instead of shifting every letter the same amount, pick a fixed letter to change each letter to:

```
| 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 |
| m | q | z | v | p | j | w | r | s | i | o | k | g | b | a | x | n | l | f | c | e | t | y | h | u | d |
```

Example: “Hello”  Encrypted: “R”
Substitution Cipher

- Idea: similar to Caesar! Instead of shifting every letter the same amount, pick a fixed letter to change each letter to:

```

  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
  m q z v p j w r s i o k g b a x n l f c e t y h u d
```

Example: “Hello” Encrypted: “Rp”
Substitution Cipher

- Idea: similar to Caesar! Instead of shifting every letter the same amount, pick a fixed letter to change each letter to:

| 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 |
| m | q | z | v | p | j | w | r | s | i | o | k | g | b | a | x | n | l | f | c | e | t | y | h | u | d |

Example: “Hello”  Encrypted: “Rpkk”
Substitution Cipher

- Idea: similar to Caesar! Instead of shifting every letter the same amount, pick a fixed letter to change each letter to:

| 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 |
| m | q | z | v | p | j | w | r | s | i | o | k | g | b | a | x | n | l | f | c | e | t | y | h | u | d |

Example: “Hello”  Encrypted: “Rpkka”
Q: What does “neskc” decrypt to?


[D] I’m confused
Q: What does “neskc” decrypt to?


[D] I’m confused
Q: What does “neskc” decrypt to?

<table>
<thead>
<tr>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
<th>e</th>
<th>f</th>
<th>g</th>
<th>h</th>
<th>i</th>
<th>j</th>
<th>k</th>
<th>l</th>
</tr>
</thead>
<tbody>
<tr>
<td>m</td>
<td>q</td>
<td>z</td>
<td>v</td>
<td>p</td>
<td>j</td>
<td>w</td>
<td>r</td>
<td>s</td>
<td>i</td>
<td>o</td>
<td>k</td>
</tr>
<tr>
<td>g</td>
<td>b</td>
<td>a</td>
<td>x</td>
<td>n</td>
<td>l</td>
<td>f</td>
<td>c</td>
<td>e</td>
<td>t</td>
<td>y</td>
<td>h</td>
</tr>
<tr>
<td>u</td>
<td>d</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

[B] quilt

n -> q
e -> u
s -> i
k -> l
c -> t
Substitution Cipher

For this to work, Alice and Bob must meet before hand to agree on a new scrambled alphabet!
Substitution Cipher!

S XLAXAFP CA ZABFSVPL CRP NEPFCSAB, "ZMB GMZRSBPF CRSBO?" CRSF FRAEKV QPWSB YSCR VPJSBSCSABF AJ CRP GPMBSBW AJ CRP CPLGF "GMZRSBP" MBV "CRSBO." CRP VPJSBSCSABF GSWRC QP JLMGPV FA MF CA LPJKPZC FA JML MF XAffsqkp CRP BALGmk EFP AJ CRP YALVF, QEC CRSF MCCSCEVP SF VMBWPLAEF, SJ CRP GPMBSBW AJ CRP YALVF "GMZRSBP" MBV "CRSBO" MLP CA QP JAEBV QU PHMGsBSBW RAY CRPU MLP ZAGGABkU EFPV SC SF VSJSZEKC CA PFZMXP CRP ZABZKEFSAB CRMC CRP GPMBSBW MBV CRP MBFYPL CA CRP NEPFCSAB, "ZMB GMZRSBPF CRSBO?" SF CA QP FAEWRC SB M FCMCSFCSZMK FELTPU FEZR MF M WMKkEX XAKK. QEC CRSF SF MQFELV.
Substitution Cipher!

S XLAXAFP CA ZABFSVPL CRP NEPFCSAB, "ZMB GMZRSBPF CRSBO?" CRSF FRAEKV QPWSB YSCR VPJSBSCSABF AJ CRP GPMBSBW AJ CRP CPLGF "GMZRSBP" MBV "CRSBO." CRP VPJSBSCSABF GSWRC QP JLMGPV FA MF CA LPJKPZC FA JML MF XAFFSQKP CRP BALGMK EFP AJ CRP YALVF, QEC CRSF MCCSCEVP SF VMBWPLAEOF, SJ CRP GPMBSBW AJ CRP YALVF "GMZRSBP" MBV "CRSBO" MLP CA QP JAEBV QU PHMGSBSBW RAY CRPU MLP ZAGGABKU EFPV SC SF VSJJSZEKC CA PFZMXP CRP ZABZKEFSAB CRMC CRP GPMBSBW MBV CRP MBFYPL CA CRP NEPFCSAB, "ZMB GMZRSBPF CRSBO?" SF CA QP FAEWRC SB M FCMCSFCSZMK FELTPU FEZR MF M WMKKEK XAKK. QEC CRSF SF MQFELV.

Q: Can we guess any letters in here?
Substitution Cipher!

S XLAXAFP CA ZABFSVPL CRP NEPFCSAB, "ZMB GMZRSBPFF CRSBO?"
CRSF FRAEKV QPWSB YSCR VPJSBSCSABF AJ CRP GPMBSBW AJ CRP
CPLGF "GMZRSBP" MBV "CRSBO." CRP VPJSBSCSABF GSWRC QP
JLMGPV FA MF CA LPJKPZC FA JML MF XAFFSQKP CRP BALGMK EFP
AJ CRP YALVF, QEC CRSF MCCSCEVP SF VMBWPLAEF, SJ CRP
GPMBSBW AJ CRP YALVF "GMZRSBP" MBV "CRSBO" MLP CA QP JAEBV
QU PHMGSBSBW RAY CRPU MLP ZAGGABKU EFPV SC SF VSJJSZEKC
CA PFZMXP CRP ZABZKEFSAB CRMC CRP GPMBSBW MBV CRP
MBFYPL CA CRP NEPFCSAB, "ZMB GMZRSBPFF CRSBO?" SF CA QP
FAEWRC SB M FCMCSFCSZMK FELTPU FEZR MF M WMKKEK XAKK.
QEC CRSF SF MQFELV.

Q: Can we guess any letters in here?

“S” is probably “A” or “I”, but otherwise…?
Substitution Cipher!

New strategy for breaking the substitution cipher:

› Q: What are the most frequently occurring letters in English?

› A: E, A, I, T, S, etc.
New strategy for breaking the substitution cipher:

- Q: What are the most frequently occurring letters in English?
- A: E, A, I, T, S, etc.

Idea: track the frequency of the encrypted letters!
Frequency Analysis

Frequency Analysis

- Determine the frequency of each encrypted letter
- Compare to the frequencies of regular English letters
- Guess the substitution alphabet
Frequency Analysis

- Determine the frequency of each *encrypted* letter
- Compare to the frequencies of regular English letters
- Guess the substitution alphabet
- The more encrypted text we see, the more accurate our encryption counts become
Frequency Analysis

- Biggest takeaway for frequency analysis: any substitution/transposition style cipher that uses the same key/shift value is breakable.

  - No more Caesar Cipher
  - No more Substitution Cipher
Frequency Analysis

Solution: we can use something like Substitution Cipher but with no repetition, so frequency analysis fails.

Idea: Instead of sharing a single shift (a la Caesar Shift), share a shift per each letter in your message.
One Time Pad

• Suppose I want to send a 13 character message: “To be or not to be”
One Time Pad

- Suppose I want to send a 13 character message: “To be or not to be”

- Provide 13 unique shifts:

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>4</td>
<td>2</td>
<td>8</td>
<td>9</td>
<td>3</td>
<td>1</td>
<td>0</td>
<td>22</td>
<td>11</td>
<td>4</td>
<td>6</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>
One Time Pad

› Suppose I want to send a 13 character message: “To be or not to be”

› Provide 13 unique shifts:

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>4</td>
<td>2</td>
<td>8</td>
<td>9</td>
<td>3</td>
<td>1</td>
<td>0</td>
<td>22</td>
<td>11</td>
<td>4</td>
<td>6</td>
<td>1</td>
</tr>
</tbody>
</table>

› Shift the 1st character of the message by the 1st shift, the second character by the 2nd, and so on!
One Time Pad

- Suppose I want to send a 13 character message: “To be or not to be”

- Provide 13 unique shifts:

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>4</td>
<td>2</td>
<td>8</td>
<td>9</td>
<td>3</td>
<td>1</td>
<td>0</td>
<td>22</td>
<td>11</td>
<td>4</td>
<td>6</td>
<td>1</td>
</tr>
</tbody>
</table>

“T” shifted by 12, “o” shifted by 4, etc.
One Time Pad

- Suppose I want to send a 13 character message: “To be or not to be”

- Provide 13 unique shifts:

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>4</td>
<td>2</td>
<td>8</td>
<td>9</td>
<td>3</td>
<td>1</td>
<td>0</td>
<td>22</td>
<td>11</td>
<td>4</td>
<td>6</td>
<td>1</td>
</tr>
</tbody>
</table>

- Frequency analysis (and similar methods) won’t work! So long as you only use the shifts once.
One Time Pad

- Major draw back one: need a secret key (the shifts) of the same length as your message (or longer) to be exchanged in advance.

- Major draw back two: need a new secret key *each time!*
Recap

- Alice, Bob, and Eve!

Q: If Alice and Bob *know* Eve may eavesdrop, how can Alice send the message so Bob can still read it?
Recap

- Alice, Bob, and Eve!

- Classical Approaches:
  - Caesar Cipher: encrypt messages by shifting lets forward an agreed upon amount
Recap

- Alice, Bob, and Eve!

- Classical Approaches:
  - Caesar Cipher
  - Substitution Cipher: generate a scrambled alphabet for encryption
Recap

- Alice, Bob, and Eve!
- Classical Approaches:
  - Caesar Cipher
  - Substitution Cipher
  - Frequency Analysis: Can break these methods with simple techniques!
Recap

- Alice, Bob, and Eve!
- Classical Approaches:
  - Caesar Cipher
  - Substitution Cipher
  - Frequency Analysis
  - One time pad: except for the one time pad. But there are many draw backs :/
- Next Time: Modern approaches that have mathematical justification for being secure!