BILL, RECORD LECTURE!!!!

BILL RECORD LECTURE!!!!
The Shift Cipher (cont)
A Caveat on Cracking The Shift Cipher

We used the following reasoning:
A Caveat on Cracking The Shift Cipher

We used the following reasoning:

1. \( f_E \cdot f_E \sim 0.065 \).
2. For \( 1 \leq i \leq 25 \), \( f_i \) is English shifted by \( i \). \( f_E \cdot f_i \sim 0.035 \).
A Caveat on Cracking The Shift Cipher

We used the following reasoning:

1. $f_E \cdot f_E \sim 0.065$.
2. For $1 \leq i \leq 25$, $f_i$ is English shifted by $i$. $f_E \cdot f_i \sim 0.035$.
3. Find correct shift $i$ by seeing which $f_E \cdot f_i$ is $\sim 0.065$. 

Did we really need the numbers $0.068$ and $0.035$? Do we actually need them? This will come up later in the course in a situation where finding the numbers is hard.
A Caveat on Cracking The Shift Cipher

We used the following reasoning:

1. $f_E \cdot f_E \sim 0.065$.
2. For $1 \leq i \leq 25$, $f_i$ is English shifted by $i$. $f_E \cdot f_i \sim 0.035$.
3. Find correct shift $i$ by seeing which $f_E \cdot f_i$ is $\sim 0.065$.
4. Only one of the dot products will be close to 0.065.
We used the following reasoning:

1. \( f_E \cdot f_E \sim 0.065 \).
2. For \( 1 \leq i \leq 25 \), \( f_i \) is English shifted by \( i \). \( f_E \cdot f_i \sim 0.035 \).
3. Find correct shift \( i \) by seeing which \( f_E \cdot f_i \) is \( \sim 0.065 \).
4. Only one of the dot products will be close to 0.065.

Did we really need the numbers 0.068 and 0.035? Do we actually need them?

This will come up later in the course in a situation where finding the numbers is hard.
How we Would Crack Shift If Did Not Know Parameters 0.065, 0.035

Important point is that $f_E \cdot f_E$ is BIG, $f_E \cdot f_i$ SMALL. Do not need to know HOW BIG, HOW SMALL.

1. Input($T$). $T$ is a text that has been coded by the shift cipher.

2. For $0 \leq i \leq 25$ find $f_i$, the freq vector of the $T$ shifted by $i$.

3. Compute all $f_E \cdot f_i$. The $i$ that has MAX of $f_E \cdot f_i$ is the $i$ we want.

Note Didn’t need the parameters 0.065, 0.035 to do this.

Downside Since we knew the parameters 0.065, 0.035 we knew there was a big gap. We knew there would be no close calls. If we do not know these kind of parameters then we are not as confident.

But if we have a few candidates for IS-ENGLISH there may be other ways to pick out the real one.
How we Would Crack Shift If Did Not Know Parameters 0.065, 0.035

Important point is that $f_E \cdot f_E$ is BIG, $f_E \cdot f_i$ SMALL. Do not need to know HOW BIG, HOW SMALL.

1. Input($T$). $T$ is a text that has been coded by the shift cipher.
Important point is that $f_E \cdot f_E$ is BIG, $f_E \cdot f_i$ SMALL. Do not need to know HOW BIG, HOW SMALL.

1. Input ($T$). $T$ is a text that has been coded by the shift cipher.
2. For $0 \leq i \leq 25$ find $f_i$, the freq vector of the $T$ shifted by $i$. 
How we Would Crack Shift If Did Not Know Parameters 0.065, 0.035

Important point is that $f_E \cdot f_E$ is BIG, $f_E \cdot f_i$ SMALL. Do not need to know HOW BIG, HOW SMALL.

1. Input($T$). $T$ is a text that has been coded by the shift cipher.
2. For $0 \leq i \leq 25$ find $f_i$, the freq vector of the $T$ shifted by $i$.
3. Compute all $f_E \cdot f_i$. The $i$ that has MAX of $f_E \cdot f_i$ is the $i$ we want.

Note Didn't need the parameters 0.065, 0.035 to do this.

Downside Since we knew the parameters 0.065, 0.035 we knew there was a big gap. We knew there would be no close calls. If we do not know these kind of parameters then we are not as confident. But if we have a few candidates for IS-ENGLISH there may be other ways to pick out the real one.
How we Would Crack Shift If Did Not Know Parameters 0.065, 0.035

Important point is that $f_E \cdot f_E$ is BIG, $f_E \cdot f_i$ SMALL. Do not need to know HOW BIG, HOW SMALL.

1. Input($T$). $T$ is a text that has been coded by the shift cipher.
2. For $0 \leq i \leq 25$ find $f_i$, the freq vector of the $T$ shifted by $i$.
3. Compute all $f_E \cdot f_i$. The $i$ that has MAX of $f_E \cdot f_i$ is the $i$ we want.

Note Didn’t need the parameters 0.065, 0.035 to do this.
How we Would Crack Shift If Did Not Know Parameters 0.065, 0.035

Important point is that $f_E \cdot f_E$ is BIG, $f_E \cdot f_i$ SMALL. Do not need to know HOW BIG, HOW SMALL.

1. Input($T$). $T$ is a text that has been coded by the shift cipher.
2. For $0 \leq i \leq 25$ find $f_i$, the freq vector of the $T$ shifted by $i$.
3. Compute all $f_E \cdot f_i$. The $i$ that has MAX of $f_E \cdot f_i$ is the $i$ we want.

Note Didn’t need the parameters 0.065, 0.035 to do this.

Downside Since we knew the parameters 0.065, 0.035 we knew there was a big gap. We knew there would be no close calls. If we do not know these kind of parameters then we are not as confident.
How we Would Crack Shift If Did Not Know Parameters 0.065, 0.035

Important point is that $f_E \cdot f_E$ is BIG, $f_E \cdot f_i$ SMALL. Do not need to know HOW BIG, HOW SMALL.

1. Input($T$). $T$ is a text that has been coded by the shift cipher.

2. For $0 \leq i \leq 25$ find $f_i$, the freq vector of the $T$ shifted by $i$.

3. Compute all $f_E \cdot f_i$. The $i$ that has MAX of $f_E \cdot f_i$ is the $i$ we want.

Note Didn’t need the parameters 0.065, 0.035 to do this.

Downside Since we knew the parameters 0.065, 0.035 we knew there was a big gap. We knew there would be no close calls. If we do not know these kind of parameters then we are not as confident.

But if we have a few candidates for IS-ENGLISH there may be other ways to pick out the real one.
Variants of the Shift Cipher
What About Texts With Numbers?

We have discussed English texts with $\Sigma = \{a, \ldots, z\}$.
What About Texts With Numbers?

We have discussed English texts with $\Sigma = \{a, \ldots, z\}$.

What if the text has numbers in it? Examples:
What About Texts With Numbers?

We have discussed English texts with \( \Sigma = \{a, \ldots, z\} \).

What if the text has numbers in it? Examples:

1. Financial Documents. \( \Sigma = \{a, b, \ldots, z, 0, \ldots, 9\} \).
What About Texts With Numbers?

We have discussed English texts with $\Sigma = \{a, \ldots, z\}$.

What if the text has numbers in it? Examples:

1. Financial Documents. $\Sigma = \{a, b, \ldots, z, 0, \ldots, 9\}$.

2. Math books such as:

   https://www.amazon.com/
   Mathematical-Muffin-Morsels-Problem-Mathematics/ 
   dp/9811215979/ref=sr_1_2?dchild=1&keywords= 
   gasarch&qid=1593879329&sr=8-2

   $\Sigma = \{a, \ldots, z, 0, \ldots, 9, +, \times, -, \div, =, \equiv, <, >, \cap, \cup, \emptyset\}$

Include other symbols depending on the branch of math. E.g.,
$\land, \lor$ for logic.
What About Texts With Numbers?

We have discussed English texts with $\Sigma = \{a, \ldots, z\}$.

What if the text has numbers in it? Examples:

1. Financial Documents. $\Sigma = \{a, b, \ldots, z, 0, \ldots, 9\}$.
2. Math books such as:

   https://www.amazon.com/
   Mathematical-Muffin-Morsels-Problem-Mathematics/
   dp/9811215979/ref=sr_1_2?dchild=1&keywords=
   gasarch&qid=1593879329&sr=8-2

   \[\Sigma = \{a, \ldots, z, 0, \ldots, 9, +, \times, -, \div, =, \equiv, <, >, \cap, \cup, \emptyset\}\]

   Include other symbols depending on the branch of math. E.g.,
   $\land, \lor$ for logic.

What to do? Find distribution of alphabet for these types of docs. Write code sim to Is-English and try all shifts.
Is Shift Cipher Secure if we are Transmitting Just Numbers?

What if Alice sends Bob a credit card number? Discuss
Is Shift Cipher Secure if we are Transmitting Just Numbers?

What if Alice sends Bob a credit card number? Discuss

Credit Card Numbers also have patterns:
Is Shift Cipher Secure if we are Transmitting Just Numbers?

What if Alice sends Bob a credit card number? Discuss
Credit Card Numbers also have patterns:

Is Shift Cipher Secure if we are Transmitting Just Numbers?

What if Alice sends Bob a credit card number? Discuss
Credit Card Numbers also have patterns:

2. American Express always begins 34 or 37.
Is Shift Cipher Secure if we are Transmitting Just Numbers?

What if Alice sends Bob a credit card number? Discuss
Credit Card Numbers also have patterns:

2. American Express always begins 34 or 37.
3. Mastercard starts with 51 or 52 or 53 or 54.
Is Shift Cipher Secure if we are Transmitting Just Numbers?

What if Alice sends Bob a credit card number? Discuss

Credit Card Numbers also have patterns:

2. American Express always begins 34 or 37.
3. Mastercard starts with 51 or 52 or 53 or 54.
4. Parity Checks.
Byte-wise Shift Cipher

- In ASCII all small letters, cap letters, numbers, punctuation, mapped to 8-bit strings.
- Use XOR instead of modular addition. Fast!
- Decode and Encode are both XOR.
- Essential properties still hold.
<table>
<thead>
<tr>
<th>Hex</th>
<th>Dec</th>
<th>Char</th>
<th>Hex</th>
<th>Dec</th>
<th>Char</th>
<th>Hex</th>
<th>Dec</th>
<th>Char</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x00</td>
<td>0</td>
<td>NULL</td>
<td>0x20</td>
<td>32</td>
<td>Space</td>
<td>0x40</td>
<td>64</td>
<td>@</td>
</tr>
<tr>
<td>0x01</td>
<td>1</td>
<td>SOH Start of heading</td>
<td>0x21</td>
<td>33</td>
<td>!</td>
<td>0x41</td>
<td>65</td>
<td>A</td>
</tr>
<tr>
<td>0x02</td>
<td>2</td>
<td>STX Start of text</td>
<td>0x22</td>
<td>34</td>
<td>&quot;</td>
<td>0x42</td>
<td>66</td>
<td>B</td>
</tr>
<tr>
<td>0x03</td>
<td>3</td>
<td>ETX End of text</td>
<td>0x23</td>
<td>35</td>
<td>#</td>
<td>0x43</td>
<td>67</td>
<td>C</td>
</tr>
<tr>
<td>0x04</td>
<td>4</td>
<td>EOT End of transmission</td>
<td>0x24</td>
<td>36</td>
<td>$</td>
<td>0x44</td>
<td>68</td>
<td>D</td>
</tr>
<tr>
<td>0x05</td>
<td>5</td>
<td>ENQ Enquiry</td>
<td>0x25</td>
<td>37</td>
<td>%</td>
<td>0x45</td>
<td>69</td>
<td>E</td>
</tr>
<tr>
<td>0x06</td>
<td>6</td>
<td>ACK Acknowledge</td>
<td>0x26</td>
<td>38</td>
<td>&amp;</td>
<td>0x46</td>
<td>70</td>
<td>F</td>
</tr>
<tr>
<td>0x07</td>
<td>7</td>
<td>BELL Bell</td>
<td>0x27</td>
<td>39</td>
<td>'</td>
<td>0x47</td>
<td>71</td>
<td>G</td>
</tr>
<tr>
<td>0x08</td>
<td>8</td>
<td>BS Backspace</td>
<td>0x28</td>
<td>40</td>
<td>(</td>
<td>0x48</td>
<td>72</td>
<td>H</td>
</tr>
<tr>
<td>0x09</td>
<td>9</td>
<td>TAB Horizontal tab</td>
<td>0x29</td>
<td>41</td>
<td>)</td>
<td>0x49</td>
<td>73</td>
<td>I</td>
</tr>
<tr>
<td>0x0A</td>
<td>10</td>
<td>LF New line</td>
<td>0x2A</td>
<td>42</td>
<td>*</td>
<td>0x4A</td>
<td>74</td>
<td>J</td>
</tr>
<tr>
<td>0x0B</td>
<td>11</td>
<td>VT Vertical tab</td>
<td>0x2B</td>
<td>43</td>
<td>+</td>
<td>0x4B</td>
<td>75</td>
<td>K</td>
</tr>
<tr>
<td>0x0C</td>
<td>12</td>
<td>FF Form Feed</td>
<td>0x2C</td>
<td>44</td>
<td>,</td>
<td>0x4C</td>
<td>76</td>
<td>L</td>
</tr>
<tr>
<td>0x0D</td>
<td>13</td>
<td>CR Carriage return</td>
<td>0x2D</td>
<td>45</td>
<td>-</td>
<td>0x4D</td>
<td>77</td>
<td>M</td>
</tr>
<tr>
<td>0x0E</td>
<td>14</td>
<td>SO Switch out</td>
<td>0x2E</td>
<td>46</td>
<td>.</td>
<td>0x4E</td>
<td>78</td>
<td>N</td>
</tr>
<tr>
<td>0x0F</td>
<td>15</td>
<td>SI Shift in</td>
<td>0x2F</td>
<td>47</td>
<td>/</td>
<td>0x4F</td>
<td>79</td>
<td>O</td>
</tr>
<tr>
<td>0x10</td>
<td>16</td>
<td>DLE Data link escape</td>
<td>0x30</td>
<td>48</td>
<td>0</td>
<td>0x50</td>
<td>80</td>
<td>P</td>
</tr>
<tr>
<td>0x11</td>
<td>17</td>
<td>DC1 Device control 1</td>
<td>0x31</td>
<td>49</td>
<td>1</td>
<td>0x51</td>
<td>81</td>
<td>Q</td>
</tr>
<tr>
<td>0x12</td>
<td>18</td>
<td>DC2 Device control 2</td>
<td>0x32</td>
<td>50</td>
<td>2</td>
<td>0x52</td>
<td>82</td>
<td>R</td>
</tr>
<tr>
<td>0x13</td>
<td>19</td>
<td>DC3 Device control 3</td>
<td>0x33</td>
<td>51</td>
<td>3</td>
<td>0x53</td>
<td>83</td>
<td>S</td>
</tr>
<tr>
<td>0x14</td>
<td>20</td>
<td>DC4 Device control 4</td>
<td>0x34</td>
<td>52</td>
<td>4</td>
<td>0x54</td>
<td>84</td>
<td>T</td>
</tr>
<tr>
<td>0x15</td>
<td>21</td>
<td>NAK Negative ack</td>
<td>0x35</td>
<td>53</td>
<td>5</td>
<td>0x55</td>
<td>85</td>
<td>U</td>
</tr>
<tr>
<td>0x16</td>
<td>22</td>
<td>SYN Synchronous idle</td>
<td>0x36</td>
<td>54</td>
<td>6</td>
<td>0x56</td>
<td>86</td>
<td>V</td>
</tr>
<tr>
<td>0x17</td>
<td>23</td>
<td>ETB End transmission block</td>
<td>0x37</td>
<td>55</td>
<td>7</td>
<td>0x57</td>
<td>87</td>
<td>W</td>
</tr>
<tr>
<td>0x18</td>
<td>24</td>
<td>CAN Cancel</td>
<td>0x38</td>
<td>56</td>
<td>8</td>
<td>0x58</td>
<td>88</td>
<td>X</td>
</tr>
<tr>
<td>0x19</td>
<td>25</td>
<td>EM End of medium</td>
<td>0x39</td>
<td>57</td>
<td>9</td>
<td>0x59</td>
<td>89</td>
<td>Y</td>
</tr>
<tr>
<td>0x1A</td>
<td>26</td>
<td>SUB Substitute</td>
<td>0x3A</td>
<td>58</td>
<td>:</td>
<td>0x5A</td>
<td>90</td>
<td>Z</td>
</tr>
<tr>
<td>0x1B</td>
<td>27</td>
<td>FSC Escape</td>
<td>0x3B</td>
<td>59</td>
<td>;</td>
<td>0x5B</td>
<td>91</td>
<td>]</td>
</tr>
<tr>
<td>0x1C</td>
<td>28</td>
<td>FS File separator</td>
<td>0x3C</td>
<td>60</td>
<td>&lt;</td>
<td>0x5C</td>
<td>92</td>
<td>\</td>
</tr>
<tr>
<td>0x1D</td>
<td>29</td>
<td>GS Group separator</td>
<td>0x3D</td>
<td>61</td>
<td>=</td>
<td>0x5D</td>
<td>93</td>
<td>]</td>
</tr>
<tr>
<td>0x1E</td>
<td>30</td>
<td>RS Record separator</td>
<td>0x3E</td>
<td>62</td>
<td>&gt;</td>
<td>0x5E</td>
<td>94</td>
<td>^</td>
</tr>
<tr>
<td>0x1F</td>
<td>31</td>
<td>US Unit separator</td>
<td>0x3F</td>
<td>63</td>
<td>?</td>
<td>0x5F</td>
<td>95</td>
<td>_</td>
</tr>
</tbody>
</table>

Byte-wise shift cipher

\[ M = \{ \text{strings of bytes} \} \]
Byte-wise shift cipher

- $\mathcal{M} = \{\text{strings of bytes}\}$

- $Gen$: choose uniform byte $k \in \mathcal{K} = \{0, \ldots, 255\}$
Byte-wise shift cipher

- $\mathcal{M} = \{\text{strings of bytes}\}$

- $Gen$: choose uniform byte $k \in \mathcal{K} = \{0, \ldots, 255\}$

- $Enc_k(m_1 \ldots m_t)$: output $c_1 \ldots c_t$, where $c_i \leftarrow m_i \oplus k$

- Verify that correctness holds.

- Curiosity: Encrypt and Decrypt Key are the same.
Byte-wise shift cipher

- $\mathcal{M} = \{\text{strings of bytes}\}$

- Gen: choose uniform byte $k \in \mathcal{K} = \{0, \ldots, 255\}$

- $Enc_k(m_1 \ldots m_t)$: output $c_1 \ldots c_t$, where $c_i \leftarrow m_i \oplus k$

- $Dec_k(c_1 \ldots c_t)$: output $m_1 \ldots m_t$, where $m_i \leftarrow c_i \oplus k$

Verify that correctness holds.

Curiosity: Encrypt and Decrypt Key are the same.
Byte-wise shift cipher

- $\mathcal{M} = \{\text{strings of bytes}\}$

- $\textbf{Gen}$: choose uniform byte $k \in \mathcal{K} = \{0, \ldots, 255\}$

- $\textbf{Enc}_k(m_1 \ldots m_t)$: output $c_1 \ldots c_t$, where $c_i \leftarrow m_i \oplus k$

- $\textbf{Dec}_k(c_1 \ldots c_t)$: output $m_1 \ldots m_t$, where $m_i \leftarrow c_i \oplus k$

- Verify that correctness holds.
Byte-wise shift cipher

- \( M = \{\text{strings of bytes}\} \)

- \( \text{Gen}: \) choose uniform byte \( k \in K = \{0, \ldots, 255\} \)

- \( \text{Enc}_k(m_1 \ldots m_t): \) output \( c_1 \ldots c_t \), where \( c_i \leftarrow m_i \oplus k \)

- \( \text{Dec}_k(c_1 \ldots c_t): \) output \( m_1 \ldots m_t \), where \( m_i \leftarrow c_i \oplus k \)

- Verify that correctness holds.

- Curiosity: Encrypt and Decrypt Key are the same.
Key is **11001110**.  
Alice wants to send **00011010**, **11100011**, **00000000**.  
She sends  
\[00011010 \oplus 11001110\]  
\[11100011 \oplus 11001110\]  
\[00000000 \oplus 11001110\]  
\[= 11010100, 00101101, 11001110\]
Example

Key is \textbf{11001110}.

Alice wants to send \textbf{00011010}, \textbf{11100011}, \textbf{00000000}.

She sends

\begin{align*}
00011010 & \oplus 11001110 \\
11100011 & \oplus 11001110 \\
00000000 & \oplus 11001110
\end{align*}

\[= 11010100, 00101101, 11001110\]

**Question:** Should it worry Alice and Bob that the key itself was transmitted? \textbf{Discuss}
Example

Key is 11001110. Alice wants to send 00011010, 11100011, 00000000. She sends

00011010 \oplus 11001110
11100011 \oplus 11001110
00000000 \oplus 11001110

= 11010100, 00101101, 11001110

Question: Should it worry Alice and Bob that the key itself was transmitted? Discuss
No. Eve has no way of knowing that.
Is this Cipher Secure?

- Today NO—only 256 possible keys!
Is this Cipher Secure?

- Today NO—only 256 possible keys!
- 100 years ago might have been secure.

- Byte is more secure—More Keys.
- Byte is less secure—uses punctuation which yields more patterns.

I do not know the answer.
Is this Cipher Secure?

- Today NO—only 256 possible keys!
- 100 years ago might have been secure.
- Given a ciphertext, try decrypting with every possible key.

What is more secure: 26-letter shift or the 256-keys Byte Shift.

- Byte is more secure—More Keys.
- Byte is less secure—uses punctuation which yields more patterns.

I do not know the answer.
Is this Cipher Secure?

- Today NO—only 256 possible keys!
- 100 years ago might have been secure.
- Given a ciphertext, try decrypting with every possible key.
- If ciphertext is long enough, only one plaintext will look like English.

What is more secure: 26-letter shift or the 256-keys Byte Shift.

- Byte is more secure- More Keys.
- Byte is less secure- uses punctuation which yields more patterns.

I do not know the answer.
Is this Cipher Secure?

- Today NO—only 256 possible keys!
- 100 years ago might have been secure.
- Given a ciphertext, try decrypting with every possible key.
- If ciphertext is long enough, only one plaintext will look like English.

What is more secure: 26-letter shift or the 256-keys Byte Shift.
Is this Cipher Secure?

- Today NO—only 256 possible keys!
- 100 years ago might have been secure.
- Given a ciphertext, try decrypting with every possible key.
- If ciphertext is long enough, only one plaintext will look like English.

What is more secure: 26-letter shift or the 256-keys Byte Shift.
- Byte is more secure- More Keys.
Is this Cipher Secure?

- Today NO—only 256 possible keys!
- 100 years ago might have been secure.
- Given a ciphertext, try decrypting with every possible key.
- If ciphertext is long enough, only one plaintext will look like English.

What is more secure: 26-letter shift or the 256-keys Byte Shift.

- Byte is more secure- More Keys.
- Byte is less secure- uses punctuation which yields more patterns.
Is this Cipher Secure?

- Today NO—only 256 possible keys!
- 100 years ago might have been secure.
- Given a ciphertext, try decrypting with every possible key.
- If ciphertext is long enough, only one plaintext will look like English.

What is more secure: 26-letter shift or the 256-keys Byte Shift.

- Byte is more secure- More Keys.
- Byte is less secure- uses punctuation which yields more patterns.
- I do not know the answer.
Sufficient Key Space Principle

- The key space must be large enough to make exhaustive-search attacks impractical.
  - How large this is may be technology-dependent.
Sufficient Key Space Principle

- The key space must be large enough to make exhaustive-search attacks impractical.
  - How large this is may be technology-dependent.

- Note: this makes some assumptions...
  - English-language plaintext
  - Ciphertext sufficiently long so only one valid plaintext
Kerckhoff’s Principle
Kerckhoff’s principle

We made the comment We KNOW that SHIFT was used.
More generally we will always use the following assumption.

Kerckhoff’s principle:

- Eve knows The encryption scheme.
- Eve knows the alphabet and the language.
- Eve does not know the key
- The key is chosen at random.
Arguments For And Against Kerckhoff’s Principle

**Arguments For:**

- Easier to keep *key* secret than *algorithm*.
- Easier to change *key* than to change *algorithm*.
- Standardization:
  - Ease of deployment.
  - Public validation.
- If prove system secure then very strong proof of security since even if Eve knows scheme she can’t crack.
Arguments For And Against Kerckhoff’s Principle

Arguments For:

- Easier to keep key secret than algorithm.
- Easier to change key than to change algorithm.
- Standardization:
  - Ease of deployment.
  - Public validation.
- If prove system secure then very strong proof of security since even if Eve knows scheme she can’t crack.

Arguments Against:

- The first few years (months? days? hours?) of a new type of cipher, perhaps you can use that Eve does not know it. But she will soon!
Formal Security with Shift Cipher as Example
1-Letter Shift Cipher

Odd Situation What if message is only one-letter long?
Discuss Can Eve crack a one-letter message?
Odd Situation What if message is only one-letter long? 
Discuss Can Eve crack a one-letter message? 
Intuitively No Eve cannot crack it.
1-Letter Shift Cipher

**Odd Situation** What if message is only one-letter long?
**Discuss** Can Eve crack a one-letter message?
**Intuitively** No Eve cannot crack it. This is correct.
1-Letter Shift Cipher

**Odd Situation** What if message is only one-letter long?
**Discuss** Can Eve crack a one-letter message?
**Intuitively** No Eve cannot crack it. This is correct.
**Discuss** How to define *secure*?
TE Means Thought Experiment

We are going to do Thought Experiments.
TE Means Thought Experiment

We are going to do Thought Experiments.

For reasons of space I call them TE.
Convention

- $m \in \{x, y\}$ is the message Alice wants to send
- $s \in \{0, 1\}$ is the shift.
- $c \in \{x, y\}$ is what Alice sends.

The statement

\[
\text{Alice sends } m + s
\]

means that that Alice sends $m$ shifted by $s$ (with wrap around).
Convention

- $m \in \{x, y\}$ is the message Alice wants to send
- $s \in \{0, 1\}$ is the shift.
- $c \in \{x, y\}$ is what Alice sends.

The statement

\[ Alice \text{ sends } m + s \]

means that Alice sends $m$ shifted by $s$ (with wrap around).
(TE1) \( \{x, y\} \), Equally Likely; Shift 0,1 Equally Likely

\[
\Pr(m = x) = \Pr(m = y) = \frac{1}{2}. \quad \Pr(s = 0) = \Pr(s = 1) = \frac{1}{2}.
\]
(TE1) \( \{x, y\} \), Equally Likely; Shift 0,1 Equally Likely

\[ \Pr(m = x) = \Pr(m = y) = \frac{1}{2}. \quad \Pr(s = 0) = \Pr(s = 1) = \frac{1}{2}. \]

<table>
<thead>
<tr>
<th>( m )</th>
<th>( s )</th>
<th>( c )</th>
<th>( \Pr )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( x )</td>
<td>0</td>
<td>( x )</td>
<td>1/4</td>
</tr>
<tr>
<td>( x )</td>
<td>1</td>
<td>( y )</td>
<td>1/4</td>
</tr>
<tr>
<td>( y )</td>
<td>0</td>
<td>( y )</td>
<td>1/4</td>
</tr>
<tr>
<td>( y )</td>
<td>1</td>
<td>( x )</td>
<td>1/4</td>
</tr>
</tbody>
</table>
\((\text{TE}1)\) \(\{x, y\}\), Equally Likely; Shift 0,1 Equally Likely

\[
\Pr(m = x) = \Pr(m = y) = \frac{1}{2}. \quad \Pr(s = 0) = \Pr(s = 1) = \frac{1}{2}.
\]

\[
\begin{array}{|c|c|c|c|}
\hline
m & s & c & \Pr \\
\hline
x & 0 & x & 1/4 \\
x & 1 & y & 1/4 \\
y & 0 & y & 1/4 \\
y & 1 & x & 1/4 \\
\hline
\end{array}
\]

Before Alice sends \(c = m + s\) Eve knows:
(TE1) \( \{x, y\} \), Equally Likely; Shift 0,1 Equally Likely

$$\Pr(m = x) = \Pr(m = y) = \frac{1}{2}.$$ \(\Pr(s = 0) = \Pr(s = 1) = \frac{1}{2}\).

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>(m)</td>
<td>(s)</td>
<td>(c)</td>
<td>(\Pr)</td>
</tr>
<tr>
<td>(x)</td>
<td>0</td>
<td>(x)</td>
<td>1/4</td>
</tr>
<tr>
<td>(x)</td>
<td>1</td>
<td>(y)</td>
<td>1/4</td>
</tr>
<tr>
<td>(y)</td>
<td>0</td>
<td>(y)</td>
<td>1/4</td>
</tr>
<tr>
<td>(y)</td>
<td>1</td>
<td>(x)</td>
<td>1/4</td>
</tr>
</tbody>
</table>

Before Alice sends \(c = m + s\) Eve knows:

$$\Pr(m = x) = \frac{1}{2}, \Pr(m = y) = \frac{1}{2}.$$
Before Alice sends $c = m + s$ Eve knows:

$$\Pr(m = x) = \Pr(m = y) = \frac{1}{2}, \Pr(s = 0) = \Pr(s = 1) = \frac{1}{2}.$$
(TE1) \( \{x, y\} \), Equally Likely; Shift 0,1 Equally Likely

\[
Pr(m = x) = Pr(m = y) = \frac{1}{2}. \quad Pr(s = 0) = Pr(s = 1) = \frac{1}{2}.
\]

<table>
<thead>
<tr>
<th>(m)</th>
<th>(s)</th>
<th>(c)</th>
<th>(Pr)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(x)</td>
<td>0</td>
<td>(x)</td>
<td>(1/4)</td>
</tr>
<tr>
<td>(x)</td>
<td>1</td>
<td>(y)</td>
<td>(1/4)</td>
</tr>
<tr>
<td>(y)</td>
<td>0</td>
<td>(y)</td>
<td>(1/4)</td>
</tr>
<tr>
<td>(y)</td>
<td>1</td>
<td>(x)</td>
<td>(1/4)</td>
</tr>
</tbody>
</table>

Before Alice sends \(c = m + s\) Eve knows:

\[
Pr(m = x) = \frac{1}{2}, \quad Pr(m = y) = \frac{1}{2}
\]

Eve sees \(c = x\). Now what does she know?

<table>
<thead>
<tr>
<th>(m)</th>
<th>(s)</th>
<th>(c)</th>
<th>(Pr)</th>
<th>Not Normalized</th>
<th>Normalized</th>
</tr>
</thead>
<tbody>
<tr>
<td>(x)</td>
<td>0</td>
<td>(x)</td>
<td>(1/4)</td>
<td>(1/2)</td>
<td></td>
</tr>
<tr>
<td>(y)</td>
<td>1</td>
<td>(x)</td>
<td>(1/4)</td>
<td>(1/2)</td>
<td></td>
</tr>
</tbody>
</table>

Eve learned **nothing** from seeing \(c\). Intuitively this means **secure**.
(TE2) Alphabet \( \{x, y\} \), Unequal Prob

\[ \Pr(m = x) = \frac{1}{4}; \Pr(m = y) = \frac{3}{4}. \Pr(s = 0) = \frac{1}{2}; \Pr(s = 1) = \frac{1}{2}. \]

\[
\begin{array}{|c|c|c|c|}
\hline
m & s & c & Pr \\
\hline
x & 0 & x & 1/8 \\
x & 1 & y & 1/8 \\
y & 0 & y & 3/8 \\
y & 1 & x & 3/8 \\
\hline
\end{array}
\]

Before Alice sees \( c = m + s \) Eve knows:

\[ \Pr(m = x) = \frac{1}{4}, \Pr(m = y) = \frac{3}{4}. \]
(TE2) Alphabet \{x, y\}, Unequal Prob

\[\Pr(m = x) = \frac{1}{4}; \quad \Pr(m = y) = \frac{3}{4}. \quad \Pr(s = 0) = \frac{1}{2}; \quad \Pr(s = 1) = \frac{1}{2}.\]

<table>
<thead>
<tr>
<th>m</th>
<th>s</th>
<th>c</th>
<th>Pr</th>
</tr>
</thead>
<tbody>
<tr>
<td>x</td>
<td>0</td>
<td>x</td>
<td>1/8</td>
</tr>
<tr>
<td>x</td>
<td>1</td>
<td>y</td>
<td>1/8</td>
</tr>
<tr>
<td>y</td>
<td>0</td>
<td>y</td>
<td>3/8</td>
</tr>
<tr>
<td>y</td>
<td>1</td>
<td>x</td>
<td>3/8</td>
</tr>
</tbody>
</table>

Before Alice sees \(c = m + s\) Eve knows:

\[\Pr(m = x) = \frac{1}{4}, \quad \Pr(m = y) = \frac{3}{4}\]

Eve sees \(c = x\). Now what does she know?
(TE2) Alphabet \( \{x, y\} \), Unequal Prob

\[
\Pr(m = x) = \frac{1}{4}; \quad \Pr(m = y) = \frac{3}{4}. \quad \Pr(s = 0) = \frac{1}{2}; \quad \Pr(s = 1) = \frac{1}{2}.
\]

\[
\begin{array}{c|c|c|c}
 m & s & c & \Pr \\
\hline
 x & 0 & x & 1/8 \\
 x & 1 & y & 1/8 \\
 y & 0 & y & 3/8 \\
 y & 1 & x & 3/8 \\
\end{array}
\]

Before Alice sees \( c = m + s \) Eve knows:

\[
\Pr(m = x) = \frac{1}{4}, \quad \Pr(m = y) = \frac{3}{4}
\]

Eve sees \( c = x \). Now what does she know?

\[
\begin{array}{c|c|c|c|c|c}
 m & s & c & \Pr & \text{Not Normalized} & \Pr & \text{Normalized} \\
\hline
 x & 0 & x & 1/8 & 1/4 \\
 y & 1 & x & 3/8 & 3/4 \\
\end{array}
\]
(TE2) Alphabet \( \{x, y\} \), Unequal Prob

\[
\Pr(m = x) = \frac{1}{4}; \ \Pr(m = y) = \frac{3}{4}. \ \Pr(s = 0) = \frac{1}{2}; \ \Pr(s = 1) = \frac{1}{2}.
\]

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>(m)</td>
<td>(s)</td>
<td>(c)</td>
<td>(\Pr)</td>
</tr>
<tr>
<td>(x)</td>
<td>0</td>
<td>(x)</td>
<td>1/8</td>
</tr>
<tr>
<td>(x)</td>
<td>1</td>
<td>(y)</td>
<td>1/8</td>
</tr>
<tr>
<td>(y)</td>
<td>0</td>
<td>(y)</td>
<td>3/8</td>
</tr>
<tr>
<td>(y)</td>
<td>1</td>
<td>(x)</td>
<td>3/8</td>
</tr>
</tbody>
</table>

Before Alice sees \(c = m + s\) Eve knows:

\[
\Pr(m = x) = \frac{1}{4}, \ \Pr(m = y) = \frac{3}{4}
\]

Eve sees \(c = x\). Now what does she know?

<table>
<thead>
<tr>
<th>(m)</th>
<th>(s)</th>
<th>(c)</th>
<th>(\Pr) Not Normalized</th>
<th>(\Pr) Normalized</th>
</tr>
</thead>
<tbody>
<tr>
<td>(x)</td>
<td>0</td>
<td>(x)</td>
<td>1/8</td>
<td>1/4</td>
</tr>
<tr>
<td>(y)</td>
<td>1</td>
<td>(x)</td>
<td>3/8</td>
<td>3/4</td>
</tr>
</tbody>
</table>

Eve learned nothing from seeing \(m\). Intuitively this means secure.
(TE3) Alphabet \( \{x, y\} \), Equal Prob, Shift Biased

\[
\Pr(m = x) = \frac{1}{2}; \quad \Pr(m = y) = \frac{1}{2}. \quad \Pr(s = 0) = \frac{1}{4}, \quad \Pr(s = 1) = \frac{3}{4}.
\]
(TE3) Alphabet \{x, y\}, Equal Prob, Shift Biased

\[ \text{Pr}(m = x) = \frac{1}{2}; \text{Pr}(m = y) = \frac{1}{2}. \text{Pr}(s = 0) = \frac{1}{4}, \text{Pr}(s = 1) = \frac{3}{4}. \]

<table>
<thead>
<tr>
<th>m</th>
<th>s</th>
<th>c</th>
<th>Pr</th>
</tr>
</thead>
<tbody>
<tr>
<td>x</td>
<td>0</td>
<td>x</td>
<td>1/8</td>
</tr>
<tr>
<td>x</td>
<td>1</td>
<td>y</td>
<td>3/8</td>
</tr>
<tr>
<td>y</td>
<td>0</td>
<td>y</td>
<td>1/8</td>
</tr>
<tr>
<td>y</td>
<td>1</td>
<td>x</td>
<td>3/8</td>
</tr>
</tbody>
</table>

Before Alice sends \( c = m + s \) Eve knows:
(TE3) Alphabet \{x, y\}, Equal Prob, Shift Biased

\[ \Pr(m = x) = \frac{1}{2}; \Pr(m = y) = \frac{1}{2}. \Pr(s = 0) = \frac{1}{4}, \Pr(s = 1) = \frac{3}{4}. \]

<table>
<thead>
<tr>
<th></th>
<th>s</th>
<th>c</th>
<th>Pr</th>
</tr>
</thead>
<tbody>
<tr>
<td>x</td>
<td>0</td>
<td>x</td>
<td>1/8</td>
</tr>
<tr>
<td>x</td>
<td>1</td>
<td>y</td>
<td>3/8</td>
</tr>
<tr>
<td>y</td>
<td>0</td>
<td>y</td>
<td>1/8</td>
</tr>
<tr>
<td>y</td>
<td>1</td>
<td>x</td>
<td>3/8</td>
</tr>
</tbody>
</table>

Before Alice sends \( c = m + s \) Eve knows:

Eve sees \( c = x \). Now what does she know?

\[ \Pr(m = x) = \frac{1}{2}; \Pr(m = y) = \frac{1}{2} \]
(TE3) Alphabet \( \{x, y\} \), Equal Prob, Shift Biased

\[
\Pr(m = x) = \frac{1}{2}; \quad \Pr(m = y) = \frac{1}{2}. \quad \Pr(s = 0) = \frac{1}{4}, \quad \Pr(s = 1) = \frac{3}{4}.
\]

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>( m )</td>
<td>( s )</td>
<td>( c )</td>
<td>( \Pr )</td>
</tr>
<tr>
<td>( x )</td>
<td>0</td>
<td>( x )</td>
<td>1/8</td>
</tr>
<tr>
<td>( x )</td>
<td>1</td>
<td>( y )</td>
<td>3/8</td>
</tr>
<tr>
<td>( y )</td>
<td>0</td>
<td>( y )</td>
<td>1/8</td>
</tr>
<tr>
<td>( y )</td>
<td>1</td>
<td>( x )</td>
<td>3/8</td>
</tr>
</tbody>
</table>

Before Alice sends \( c = m + s \) Eve knows:

Eve sees \( c = x \). Now what does she know?

\[
\Pr(m = x) = \frac{1}{2}; \quad \Pr(m = y) = \frac{1}{2}
\]

Before: Eve-\( \Pr(m = x) = \frac{1}{2} \). After: Eve-\( \Pr(m = x) = \frac{1}{4} \).

Eve has learned something!
(TE3) Alphabet \( \{x, y\} \), Equal Prob, Shift Biased

\[
\Pr(m = x) = \frac{1}{2}; \, \Pr(m = y) = \frac{1}{2}. \, \Pr(s = 0) = \frac{1}{4}, \, \Pr(s = 1) = \frac{3}{4}.
\]

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Before Alice sends \( c = m + s \), Eve knows:
Eve sees \( c = x \). Now what does she know?

\[
\Pr(m = x) = \frac{1}{2}; \, \Pr(m = y) = \frac{1}{2}
\]
Eve sees \( c = x \). Now what does she know?

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Before: Eve \( \Pr(m = x) = \frac{1}{2} \). After: Eve \( \Pr(m = x) = \frac{1}{4} \).

\textit{Eve has learned something!}
BILL, RECORD LECTURE!!!!

BILL RECORD LECTURE!!!!
Upshot

Insecure does not mean Eve can find the message.

Insecure means that Eve knows more after seeing c than she did before seeing c.

What she knows might involve probability.

We need to make this all more rigorous!
Insecure does not mean Eve can find the message.

Insecure means that Eve knows more after seeing $c$ than she did before seeing $c$. What she knows might involve probability. We need to make this all more rigorous!
Insecure does not mean Eve can find the message.
Insecure means that Eve knows more after seeing $c$ than she did before seeing $c$. 
Upshot

- **Insecure** does not mean Eve can find the message.
- **Insecure** means that Eve knows more after seeing \( c \) than she did before seeing \( c \).
- What she knows might involve probability.
Insecure does not mean Eve can find the message.
Insecure means that Eve knows more after seeing \( c \) than she did before seeing \( c \).
What she knows might involve probability.
We need to make this all more rigorous!
We Need Conditional Probability

**Conditional probability** Probability that one event occurs, *given that some other event occurred.*
We Need Conditional Probability

**Conditional probability** Probability that one event occurs, *given that some other event occurred.*

**Notation** $\Pr(A|B)$. 
We Need Conditional Probability

**Conditional probability** Probability that one event occurs, *given that some other event occurred*.

**Notation** $\Pr(A|B)$.

**Formal Definition Notation**

$$ \Pr(A|B) = \frac{\Pr(A \cap B)}{\Pr(B)}.$$
We Need Conditional Probability

**Conditional probability** Probability that one event occurs, *given that some other event occurred*.

**Notation** $\Pr(A|B)$.

**Formal Definition Notation** $\Pr(A|B) = \frac{\Pr(A \cap B)}{\Pr(B)}$.

**Intuition** $\Pr(A|B) = \frac{\Pr(A \cap B)}{\Pr(B)}$ is saying that the entire space is now $\Pr(B)$. Within that space what is the prob of $A$ happening? Its $\Pr(A \cap B)$. 
Josh rolls dice $d_1, d_2$ and finds $s = d_1 + d_2$. What is $\Pr(s = 5)$?

$$\Pr(s = 5) = \frac{1}{6}.$$
Examples of Conditional Probability

Josh rolls dice $d_1, d_2$ and finds $s = d_1 + d_2$. What is $\Pr(s = 5)$? $\frac{1}{9}$. What if you know $d_1$?
Examples of Conditional Probability

Josh rolls dice $d_1, d_2$ and finds $s = d_1 + d_2$. What is $\Pr(s = 5)$? $\frac{1}{9}$. What if you know $d_1$?

$\Pr(s = 5 | d_1 = 1) = \frac{\Pr(s=5 \land d_1=1)}{\Pr(d_1=1)} = \frac{1/36}{1/6} = \frac{1}{6}$. 

This example is bad since, for example $\Pr(s = 5 | d_1 = 2) = \Pr(d_2 = 3) = \frac{1}{6}$. 

$\Pr(s = 5 | d_1 = 5) = \Pr(d_2 = 0) = 0$. 

Examples of Conditional Probability

Josh rolls dice $d_1, d_2$ and finds $s = d_1 + d_2$. What is $\Pr(s = 5)$? $\frac{1}{9}$.

What if you know $d_1$?

$\Pr(s = 5|d_1 = 1) = \frac{\Pr(s=5 \land d_1=1)}{\Pr(d_1=1)} = \frac{1/36}{1/6} = \frac{1}{6}$.

$\Pr(s = 5|d_1 = 2) = \frac{\Pr(s=5 \land d_1=2)}{\Pr(d_1=2)} = \frac{1/36}{1/6} = \frac{1}{6}$.

This example is bad since, for example $\Pr(s = 5|d_1 = 2) = \Pr(d_2 = 3) = \frac{1}{6}$.
Examples of Conditional Probability

Josh rolls dice $d_1, d_2$ and finds $s = d_1 + d_2$. What is $\Pr(s = 5)$? $\frac{1}{9}$. What if you know $d_1$?

$\Pr(s = 5|d_1 = 1) = \frac{\Pr(s=5\land d_1=1)}{\Pr(d_1=1)} = \frac{1/36}{1/6} = \frac{1}{6}$.

$\Pr(s = 5|d_1 = 2) = \frac{\Pr(s=5\land d_1=2)}{\Pr(d_1=2)} = \frac{1/36}{1/6} = \frac{1}{6}$.

$\Pr(s = 5|d_1 = 3) = \frac{\Pr(s=5\land d_1=3)}{\Pr(d_1=3)} = \frac{1/36}{1/6} = \frac{1}{6}$.

This example is bad since, for example $\Pr(s = 5|d_1 = 2) = \Pr(d_2 = 3) = \frac{1}{6}$.
Examples of Conditional Probability

Josh rolls dice $d_1, d_2$ and finds $s = d_1 + d_2$. What is $\Pr(s = 5)$? $\frac{1}{9}$. What if you know $d_1$?

$\Pr(s = 5 | d_1 = 1) = \frac{\Pr(s=5 \land d_1=1)}{\Pr(d_1=1)} = \frac{1/36}{1/6} = \frac{1}{6}$.

$\Pr(s = 5 | d_1 = 2) = \frac{\Pr(s=5 \land d_1=2)}{\Pr(d_1=2)} = \frac{1/36}{1/6} = \frac{1}{6}$.

$\Pr(s = 5 | d_1 = 3) = \frac{\Pr(s=5 \land d_1=3)}{\Pr(d_1=3)} = \frac{1/36}{1/6} = \frac{1}{6}$.

$\Pr(s = 5 | d_1 = 4) = \frac{\Pr(s=5 \land d_1=4)}{\Pr(d_1=4)} = \frac{1/36}{1/6} = \frac{1}{6}$.

This example is bad since, for example $\Pr(s = 5 | d_1 = 2) = \Pr(d_2 = 3) = \frac{1}{6}$.

$\Pr(s = 5 | d_1 = 5) = \Pr(d_2 = 0) = 0$. 
Examples of Conditional Probability

Josh rolls dice $d_1, d_2$ and finds $s = d_1 + d_2$. What is $\Pr(s = 5)$? $\frac{1}{9}$. What if you know $d_1$?

$\Pr(s = 5|d_1 = 1) = \frac{\Pr(s=5 \land d_1=1)}{\Pr(d_1=1)} = \frac{1/36}{1/6} = \frac{1}{6}$.

$\Pr(s = 5|d_1 = 2) = \frac{\Pr(s=5 \land d_1=2)}{\Pr(d_1=2)} = \frac{1/36}{1/6} = \frac{1}{6}$.

$\Pr(s = 5|d_1 = 3) = \frac{\Pr(s=5 \land d_1=3)}{\Pr(d_1=3)} = \frac{1/36}{1/6} = \frac{1}{6}$.

$\Pr(s = 5|d_1 = 4) = \frac{\Pr(s=5 \land d_1=4)}{\Pr(d_1=4)} = \frac{1/36}{1/6} = \frac{1}{6}$.

$\Pr(s = 5|d_1 = 5) = \frac{\Pr(s=5 \land d_1=5)}{\Pr(d_1=5)} = \frac{0}{1/6} = 0$. 

This example is bad since, for example $\Pr(s = 5|d_1 = 2) = \Pr(d_2=3) = \frac{1}{6}$. 

$\Pr(s = 5|d_1 = 5) = \Pr(d_2=0) = 0$. 

Examples of Conditional Probability

Josh rolls dice $d_1, d_2$ and finds $s = d_1 + d_2$. What is $\Pr(s = 5)$? $\frac{1}{9}$.

What if you know $d_1$?

\[
\Pr(s = 5|d_1 = 1) = \frac{\Pr(s=5\wedge d_1=1)}{\Pr(d_1=1)} = \frac{1/36}{1/6} = \frac{1}{6}.
\]

\[
\Pr(s = 5|d_1 = 2) = \frac{\Pr(s=5\wedge d_1=2)}{\Pr(d_1=2)} = \frac{1/36}{1/6} = \frac{1}{6}.
\]

\[
\Pr(s = 5|d_1 = 3) = \frac{\Pr(s=5\wedge d_1=3)}{\Pr(d_1=3)} = \frac{1/36}{1/6} = \frac{1}{6}.
\]

\[
\Pr(s = 5|d_1 = 4) = \frac{\Pr(s=5\wedge d_1=4)}{\Pr(d_1=4)} = \frac{1/36}{1/6} = \frac{1}{6}.
\]

\[
\Pr(s = 5|d_1 = 5) = \frac{\Pr(s=5\wedge d_1=5)}{\Pr(d_1=5)} = \frac{0}{1/6} = 0.
\]

\[
\Pr(s = 5|d_1 = 6) = \frac{\Pr(s=5\wedge d_1=6)}{\Pr(d_1=6)} = \frac{0}{1/6} = 0.
\]
Examples of Conditional Probability

Josh rolls dice $d_1, d_2$ and finds $s = d_1 + d_2$. What is $\Pr(s = 5)$? $\frac{1}{9}$.

What if you know $d_1$?

- $\Pr(s = 5|d_1 = 1) = \frac{\Pr(s=5 \land d_1=1)}{\Pr(d_1=1)} = \frac{1/36}{1/6} = \frac{1}{6}$.
- $\Pr(s = 5|d_1 = 2) = \frac{\Pr(s=5 \land d_1=2)}{\Pr(d_1=2)} = \frac{1/36}{1/6} = \frac{1}{6}$.
- $\Pr(s = 5|d_1 = 3) = \frac{\Pr(s=5 \land d_1=3)}{\Pr(d_1=3)} = \frac{1/36}{1/6} = \frac{1}{6}$.
- $\Pr(s = 5|d_1 = 4) = \frac{\Pr(s=5 \land d_1=4)}{\Pr(d_1=4)} = \frac{1/36}{1/6} = \frac{1}{6}$.
- $\Pr(s = 5|d_1 = 5) = \frac{\Pr(s=5 \land d_1=5)}{\Pr(d_1=5)} = \frac{0}{1/6} = 0$.
- $\Pr(s = 5|d_1 = 6) = \frac{\Pr(s=5 \land d_1=6)}{\Pr(d_1=6)} = \frac{0}{1/6} = 0$.

This example is bad since, for example

- $\Pr(s = 5|d_1 = 2) = \Pr(d_2 = 3) = \frac{1}{6}$.
- $\Pr(s = 5|d_1 = 5) = \Pr(d_2 = 0) = 0$. 


Josh rolls die $d$ and announces the parity.
Josh rolls die $d$ and announces the parity.

$$\Pr(d = 1|d \text{ even}) = \frac{\Pr(d = 1 \land d \equiv 0)}{\Pr(d \equiv 1)} = 0$$
Josh rolls die $d$ and announces the parity.

$$\Pr(d = 1 \mid d \text{ even}) = \frac{\Pr(d=1 \land d \equiv 0)}{\Pr(d \equiv 1)} = 0$$

$$\Pr(d = 1 \mid d \text{ odd}) = \frac{\Pr(d=1 \land d \equiv 1)}{\Pr(d \equiv 1)} = \frac{1/6}{1/2} = \frac{1}{3}$$
Josh rolls die $d$ and announces the parity.

\[ \Pr(d = 1 \mid d \text{ even}) = \frac{\Pr(d=1 \land d \equiv 0)}{\Pr(d\equiv 1)} = 0 \]

\[ \Pr(d = 1 \mid d \text{ odd}) = \frac{\Pr(d=1 \land d \equiv 1)}{\Pr(d\equiv 1)} = \frac{1/6}{1/2} = \frac{1}{3} \]

The rest are similar and are always either 0 or $\frac{1}{3}$. 
Conditional Probability Example with Funky Dice

Josh rolls two dice $d_1, d_2$ and finds $s = d_1 + d_2$. The dice are \textbf{not} independent.

$d_1$ is fair.
If $d_1$ is $i$, then $d_2 \leq i$, but within that equal prob.
If $d_1 = 3$ then $d_2$ is 1,2,3 each with prob $\frac{1}{3}$.
Conditional Probability Example with Funky Dice

Josh rolls two dice $d_1, d_2$ and finds $s = d_1 + d_2$. The dice are **not** independent.

$d_1$ is fair.

If $d_1$ is $i$, then $d_2 \leq i$, but within that equal prob.

If $d_1 = 3$ then $d_2$ is 1,2,3 each with prob $\frac{1}{3}$.

**Shortcut** $\Pr(d_1 = i \land s = 5) = \Pr(d_1 = i \land d_2 = 5 - i)$. 
Josh rolls two dice $d_1, d_2$ and finds $s = d_1 + d_2$.
The dice are not independent.
$d_1$ is fair.
If $d_1$ is $i$, then $d_2 \leq i$, but within that equal prob.
If $d_1 = 3$ then $d_2$ is 1,2,3 each with prob $\frac{1}{3}$.

**Shortcut** $\Pr(d_1 = i \land s = 5) = \Pr(d_1 = i \land d_2 = 5 - i)$.

\[
\begin{align*}
\Pr(s = 5|d_1 = 1) &= \frac{\Pr(d_1=1 \land d_2=4)}{\Pr(d_1=1)} = 0 \\
\Pr(s = 5|d_1 = 2) &= \frac{\Pr(d_1=2 \land d_2=3)}{\Pr(d_1=2)} = 0 \\
\Pr(s = 5|d_1 = 3) &= \frac{\Pr(d_1=3 \land d_2=2)}{\Pr(d_1=3)} = \frac{1/6 \times 1/3}{1/6} = \frac{1}{3} \\
\Pr(s = 5|d_1 = 4) &= \frac{\Pr(d_1=4 \land d_2=1)}{\Pr(d_1=4)} = \frac{1/6 \times 1/4}{1/6} = \frac{1}{4} \\
\Pr(s = 5|d_1 = 5) &= \frac{\Pr(d_1=5 \land d_2=0)}{\Pr(d_1=5)} = 0 \\
\Pr(s = 5|d_1 = 6) &= \frac{\Pr(d_1=5 \land d_2=-1)}{\Pr(d_1=6)} = 0.
\end{align*}
\]
Conditional Probability Example with Funky Dice

Josh rolls two dice $d_1, d_2$ and finds $s = d_1 + d_2$.
The dice are **not** independent.
$d_1$ is fair.
If $d_1$ is $i$, then $d_2 \leq i$, but within that equal prob.
If $d_1 = 3$ then $d_2$ is 1,2,3 each with prob $\frac{1}{3}$.

**Shortcut** $\Pr(d_1 = i \land s = 5) = \Pr(d_1 = i \land d_2 = 5 - i)$.

\[
\begin{align*}
\Pr(s = 5|d_1 = 1) &= \frac{\Pr(d_1=1 \land d_2=4)}{\Pr(d_1=1)} = 0 \\
\Pr(s = 5|d_1 = 2) &= \frac{\Pr(d_1=2 \land d_2=3)}{\Pr(d_1=2)} = 0 \\
\Pr(s = 5|d_1 = 3) &= \frac{\Pr(d_1=3 \land d_2=2)}{\Pr(d_1=3)} = \frac{1/6 \times 1/3}{1/6} = \frac{1}{3} \\
\Pr(s = 5|d_1 = 4) &= \frac{\Pr(d_1=4 \land d_2=1)}{\Pr(d_1=4)} = \frac{1/6 \times 1/4}{1/6} = \frac{1}{4} \\
\Pr(s = 5|d_1 = 5) &= \frac{\Pr(d_1=5 \land d_2=0)}{\Pr(d_1=5)} = 0. \\
\Pr(s = 5|d_1 = 6) &= \frac{\Pr(d_1=5 \land d_2=-1)}{\Pr(d_1=6)} = 0.
\end{align*}
\]
The rest are similar. Many are 0.
Bill has two coins F (for Fair) and B (for Biased) \( \Pr(H) = \frac{3}{4} \).
He picks one at random (using a sep fair coin).
He flips the coin.
Bill has two coins $F$ (for Fair) and $B$ (for Biased) $\Pr(H) = \frac{3}{4}$.
He picks one at random (using a separate fair coin).
He flips the coin.
$\Pr(H|B) = \frac{3}{4}$ by definition of Bias.
$\Pr(H|F) = \frac{1}{2}$ by definition of Fair.
Conditional Probability Example with a Biased Coin

Bill has two coins F (for Fair) and B (for Biased) \( \Pr(H) = \frac{3}{4} \). He picks one at random (using a sep fair coin). He flips the coin.

\[ \Pr(H|B) = \frac{3}{4} \] by definition of Bias.
\[ \Pr(H|F) = \frac{1}{2} \] by definition of Fair.

\[ \Pr(B|H) = \frac{\Pr(B \cap H)}{\Pr(H)}. \]
Conditional Probability Example with a Biased Coin

Bill has two coins F (for Fair) and B (for Biased) $\Pr(H) = \frac{3}{4}$.
He picks one at random (using a sep fair coin).
He flips the coin.
$\Pr(H|B) = \frac{3}{4}$ by definition of Bias.
$\Pr(H|F) = \frac{1}{2}$ by definition of Fair.

$\Pr(B|H) = \frac{\Pr(B \cap H)}{\Pr(H)}$.

$\Pr(B \cap H) = \Pr(B) \times \Pr(H|B) = \frac{1}{2} \times \frac{3}{4} = \frac{3}{8}$.
$\Pr(H) = \Pr(B) \times \Pr(H|B) + \Pr(F) \times \Pr(H|F) = \frac{1}{2} \times \frac{1}{2} + \frac{1}{2} \times \frac{3}{4} = \frac{5}{8}$
Bill has two coins F (for Fair) and B (for Biased) $\Pr(H) = \frac{3}{4}$.
He picks one at random (using a sep fair coin).
He flips the coin.
$\Pr(H|B) = \frac{3}{4}$ by definition of Bias.
$\Pr(H|F) = \frac{1}{2}$ by definition of Fair.

\[
\Pr(B|H) = \frac{\Pr(B \cap H)}{\Pr(H)}.
\]

\[
\Pr(B \cap H) = \Pr(B) \times \Pr(H|B) = \frac{1}{2} \times \frac{3}{4} = \frac{3}{8}.
\]
\[
\Pr(H) = \Pr(B) \times \Pr(H|B) + \Pr(F) \times \Pr(H|F) = \frac{1}{2} \times \frac{1}{2} + \frac{1}{2} \times \frac{3}{4} = \frac{5}{8}
\]

\[
\Pr(B|H) = \frac{\Pr(B \cap H)}{\Pr(H)} = \frac{3/8}{5/8} = \frac{3}{5}.
\]
Definition of a Secure Crypto System

$m$ will be a message.
Definition of a Secure Crypto System

$m$ will be a message. $c$ is what is sent. If the following holds then the system is secure.

$$(\forall m, x, y, c)[\Pr(m = x|c = y) = \Pr(m = x)].$$

So seeing the $y$ does not help Eve at all.
Definition of a Secure Crypto System

$m$ will be a message. $c$ is what is sent. If the following holds then the system is secure.

$$(\forall m, x, y, c)[\Pr(m = x|c = y) = \Pr(m = x)].$$

So seeing the $y$ does not help Eve at all.

Is this info-theoretic security or comp-security? Discuss
Definition of a Secure Crypto System

$m$ will be a message. $c$ is what is sent.
If the following holds then the system is secure.

$$(\forall m, x, y, c)[\Pr(m = x|c = y) = \Pr(m = x)].$$

So seeing the $y$ does not help Eve at all.
Is this info-theoretic security or comp-security? Discuss

Info-Theoretic  If Eve has unlimited computing power she still learns nothing.
One-Letter Shift is Secure!

Alphabet is \{x, y\}. \( s \in \{0, 1\} \) randomly.
\[ \Pr(m = x) = p_x. \quad \Pr(m = y) = p_y. \]
One-Letter Shift is Secure!

Alphabet is \{x, y\}. \(s \in \{0, 1\}\) randomly.
\(\Pr(m = x) = p_x\). \(\Pr(m = y) = p_y\). Eve knows this.
One-Letter Shift is Secure!

Alphabet is \{x, y\}. \(s \in \{0, 1\}\) randomly.
\(\Pr(m = x) = p_x\). \(\Pr(m = y) = p_y\). Eve knows this.
Note that \(p_x + p_y = 1\).
One-Letter Shift is Secure!

Alphabet is \{x, y\}. \(s \in \{0, 1\}\) randomly.
\(\Pr(m = x) = p_x\). \(\Pr(m = y) = p_y\). Eve knows this.
Note that \(p_x + p_y = 1\).

\[
\Pr(m = x | c = x) = \frac{\Pr(m = x \land c = x)}{\Pr(c = x)}
\]
One-Letter Shift is Secure!

Alphabet is \( \{x, y\} \). \( s \in \{0, 1\} \) randomly. 
\( \Pr(m = x) = p_x \). \( \Pr(m = y) = p_y \). Eve knows this.  
Note that \( p_x + p_y = 1 \).

\[
\Pr(m = x | c = x) = \frac{\Pr(m = x \land c = x)}{\Pr(c = x)}
\]

\[
\Pr(m = x \land c = x) = \Pr(m = x \land s = 0) = p_x \times \frac{1}{2} = 0.5p_x
\]
One-Letter Shift is Secure!

Alphabet is \( \{x, y\} \). \( s \in \{0, 1\} \) randomly.
\( \Pr(m = x) = p_x \). \( \Pr(m = y) = p_y \). Eve knows this. Note that \( p_x + p_y = 1 \).

\[
\Pr(m = x | c = x) = \frac{\Pr(m = x \land c = x)}{\Pr(c = x)}
\]

\[
\Pr(m = x \land c = x) = \Pr(m = x \land s = 0) = p_x \times \frac{1}{2} = 0.5p_x
\]
\[
\Pr(c = x) = \Pr(m = x)\Pr(s = 0) + \Pr(m = y)\Pr(s = 1) = 0.5p_x + 0.5p_y = 0.5(p_x + p_y)
\]
One-Letter Shift is Secure!

Alphabet is \( \{x, y\} \). \( s \in \{0, 1\} \) randomly.
\( \Pr(m = x) = p_x \). \( \Pr(m = y) = p_y \). Eve knows this.
Note that \( p_x + p_y = 1 \).

\[
\Pr(m = x | c = x) = \frac{\Pr(m = x \land c = x)}{\Pr(c = x)}
\]

\[
\Pr(m = x \land c = x) = \Pr(m = x \land s = 0) = p_x \times \frac{1}{2} = 0.5p_x
\]
\[
\Pr(c = x) = \Pr(m = x)\Pr(s = 0) + \Pr(m = y)\Pr(s = 1) = 0.5p_x + 0.5p_y = 0.5(p_x + p_y)
\]

\[
\Pr(m = x | c = x) = \frac{0.5p_x}{0.5(p_x + p_y)} = p_x
\]
One-Letter Shift is Secure! (cont)

Alphabet is \{x, y\}. \( s \in \{0, 1\} \) randomly.
\( \Pr(m = x) = p_x. \) \( \Pr(m = y) = p_y. \)
One-Letter Shift is Secure! (cont)

Alphabet is \(\{x, y\}\). \(s \in \{0, 1\}\) randomly.

\(\Pr(m = x) = p_x\). \(\Pr(m = y) = p_y\). Eve knows this.
One-Letter Shift is Secure! (cont)

Alphabet is \{x, y\}. \(s \in \{0, 1\}\) randomly.
\(\Pr(m = x) = p_x\). \(\Pr(m = y) = p_y\). Eve knows this.
Note that \(p_x + p_y = 1\).
We showed

\[
\Pr(m = x | c = x) = p_x
\]
One-Letter Shift is Secure! (cont)

Alphabet is \( \{x, y\} \). \( s \in \{0, 1\} \) randomly.
\( \Pr(m = x) = p_x \). \( \Pr(m = y) = p_y \). Eve knows this.
Note that \( p_x + p_y = 1 \).
We showed

\[
\Pr(m = x | c = x) = p_x
\]

One can show:

\[
\Pr(m = x | c = y) = p_x.
\]

\[
\Pr(m = y | c = x) = p_y.
\]

\[
\Pr(m = y | c = y) = p_y.
\]
One-Letter Shift is Secure! (cont)

Alphabet is \{x, y\}. \( s \in \{0, 1\} \) randomly. 
\( \Pr(m = x) = p_x \). \( \Pr(m = y) = p_y \). Eve knows this. 
Note that \( p_x + p_y = 1 \). 
We showed 

\[ \Pr(m = x|c = x) = p_x \]

One can show:

\[ \Pr(m = x|c = y) = p_x. \]

\[ \Pr(m = y|c = x) = p_y. \]

\[ \Pr(m = y|c = y) = p_y. \]

So seeing the ciphertext gives Eve \textbf{NO INFORMATION}. 

\textbf{Upshot} The 1-letter shift \textbf{Information-Theoretic Secure}. 
Is 2-letter Shift Uncrackable?

Is 2-letter Shift Uncrackable? Discuss.
Is 2-letter Shift Uncrackable?

Is 2-letter Shift Uncrackable? Discuss.
No. Alphabet is \{X, Y\}.
Is 2-letter Shift Uncrackable? Discuss.
No. Alphabet is \{X, Y\}.
If Eve sees XX then she knows that the original message was one of
\{XX, YY\}
So Eve has learned something. HW will make this rigorous.
Summary and a New Question

Alice and Bob use shifts: unif, 1-letter. Secure

Alice and Bob use shifts: bias, 1-letter. Insecure

Alice and Bob use shifts: unif, 2-letters. Insecure

New Question
Is the last item that important? We are saying that Eve knows prob stuff, but does she really KNOW something?
Summary and a New Question

- Alice and Bob use shift $s$ unif, 1-letter.

New Question

Is the last item that important? We are saying that Eve knows prob stuff, but does she really KNOW something?
Summary and a New Question

- Alice and Bob use shift $s$ unif, 1-letter. **Secure**
Summary and a New Question

- Alice and Bob use shift $s$ unif, 1-letter. **Secure**
- Alice and Bob use shift $s$ bias, 1-letter.
Summary and a New Question

- Alice and Bob use shift $s$ unif, 1-letter. **Secure**
- Alice and Bob use shift $s$ bias, 1-letter. **Insecure**

New Question

Is the last item that important?

We are saying that Eve knows prob stuff, but does she really **KNOW** something?
Summary and a New Question

- Alice and Bob use shift $s$ unif, 1-letter. **Secure**
- Alice and Bob use shift $s$ bias, 1-letter. **Insecure**
- Alice and Bob use shift $s$ unif, 2-letters.

New Question

Is the last item that important? We are saying that Eve knows prob stuff, but does she really KNOW something?
Summary and a New Question

- Alice and Bob use shift $s$ unif, 1-letter. **Secure**
- Alice and Bob use shift $s$ bias, 1-letter. **Insecure**
- Alice and Bob use shift $s$ unif, 2-letters. **Insecure**

New Question

Is the last item that important? We are saying that Eve knows prob stuff, but does she really KNOW something?
Summary and a New Question

- Alice and Bob use shift $s$ unif, 1-letter. **Secure**
- Alice and Bob use shift $s$ bias, 1-letter. **Insecure**
- Alice and Bob use shift $s$ unif, 2-letters. **Insecure**

**New Question** Is the last item that important?
Summary and a New Question

- Alice and Bob use shift $s$ unif, 1-letter. **Secure**
- Alice and Bob use shift $s$ bias, 1-letter. **Insecure**
- Alice and Bob use shift $s$ unif, 2-letters. **Insecure**

**New Question** Is the last item that important? We are saying that Eve knows prob stuff, but does she really KNOW something?
Can Two 1-Letter Messages Leak Information?

Can Two 1-Letter Messages using the same shift Leak Information?
Can Two 1-Letter Messages Leak Information?

Can Two 1-Letter Messages using the same shift Leak Information?
Yes
Can Two 1-Letter Messages Leak Information?

Can Two 1-Letter Messages using the same shift Leak Information?  
Yes

Scenario

Visible to all:  Is Eric a double agent working for the Klingons?
Can Two 1-Letter Messages Leak Information?

Yes

Scenario
Visible to all: Is Eric a double agent working for the Klingons?
The answer comes via a shift cipher: A (which is either Y or N)
Can Two 1-Letter Messages Leak Information?

Can Two 1-Letter Messages using the same shift Leak Information? Yes

**Scenario**
Visible to all: *Is Eric a double agent working for the Klingons?*
The answer comes via a shift cipher: A (which is either Y or N)

In clear: *Is Eric a double agent working for the Romulans?*
Can Two 1-Letter Messages Leak Information?

Yes

Scenario

Visible to all: Is Eric a double agent working for the Klingons?
The answer comes via a shift cipher: A (which is either Y or N)

In clear: Is Eric a double agent working for the Romulans?
The answer comes via a shift cipher: A (which is either Y or N)
Can Two 1-Letter Messages Leak Information?

Can Two 1-Letter Messages using the same shift Leak Information? Yes

**Scenario**
Visible to all: **Is Eric a double agent working for the Klingons?**
The answer comes via a shift cipher: **A** (which is either Y or N)

In clear: **Is Eric a double agent working for the Romulans?**
The answer comes via a shift cipher: **A** (which is either Y or N)

Since the answer to both questions was **the same**, namely A, Eve knows Eric is working for either **both** or **neither**.
Eve Can Tell if Two Message Are Same

**Issue** If Eve sees two messages, will know if they are the same or different.

**Does this leak information** Discuss.
Eve Can Tell if Two Message Are Same

**Issue** If Eve sees two messages, will know if they are the same or different.

**Does this leak information** Discuss. Yes.
Eve Can Tell if Two Message Are Same

**Issue** If Eve sees two messages, will know if they are the same or different.

**Does this leak information** Discuss. Yes.

**What to do about this?** Discuss.
Eve Can Tell if Two Messages Are Same

**Issue** If Eve sees two messages, will know if they are the same or different.

**Does this leak information** Discuss. Yes.

**What to do about this?** Discuss.

**For Now Nothing** Will come back to this issue after a few more ciphers.
Eve Can Tell if Two Messages Are Same

**Issue** If Eve sees two messages, will know if they are the same or different.

**Does this leak information** Discuss. Yes.

**What to do about this?** Discuss.

**For Now Nothing** Will come back to this issue after a few more ciphers.

**For Now** A lesson in how even defining security and leak must be done carefully.
Private-Key Encryption

\[ c := \text{Enc}_k(m) \quad \text{message/plaintext} \]

\[ m := \text{Dec}_k(c) \quad \text{decryption} \]
Private-key encryption

\[ k \quad m \quad c := \text{Enc}_k(m) \]

\[ c \quad c \quad m := \text{Dec}_k(c) \]
Private-key encryption

- A *private-key encryption scheme* is defined by a message space $\mathcal{M}$ and algorithms $(\text{Gen, Enc, Dec})$
  - **Gen** (key generation algorithm): outputs $k \in \mathcal{K}$
    (For SHIFT this is $k \in \{0, \ldots, 25\}$. Should 0 be included?)
  - **Enc** (encryption algorithm): takes key $k$ and message $m \in \mathcal{M}$ as input; outputs ciphertext $c$
    $$c \leftarrow \text{Enc}_k(m)$$
    (For SHIFT this is $\text{Enc}(m_1, \ldots, m_n) = (m_1 + k, \ldots, m_n + k)$.)
  - **Dec** (decryption algorithm): takes key $k$ and ciphertext $c$ as input; outputs $m$ or “error”
    $$m := \text{Dec}_k(c)$$
    (For SHIFT this is $\text{Dec}(c_1, \ldots, c_n) = (c_1 - k, \ldots, c_n - k)$.)
    \[ \forall k\ output\ by\ \text{Gen} \ \forall m \in \mathcal{M}, \text{Dec}_k(\text{Enc}_k(m)) = m \]
    (For SHIFT this is $(m + k) - k = m$)
BILL, STOP RECORDING LECTURE!!!!

BILL STOP RECORD LECTURE!!!