Midterm 2 (Multiple Choice Only)

Median: 88.7%
Average: 90.0%
29 Perfect Scores!
Midterm 2
FR Grading in Progress
(Grades expected on Wednesday)
Data Gathered

Visualization Proposed

Presentation Due
Lab sections this week!
Final Project

Option 1: Present a d3 visualization of your data

Option 2: Present an Excel overview sheet of your data
Presentation

Quick, 2-3 minute overview of your data and your summary. *Only your XLSX or d3.js visualization.* No PPT.
SSL
SSL
Secure Sockets Layer
SSL
Secure Sockets Layer

TLS
Transport Layer Security
TLS Provides Two Things
TLS Provides Two Things

“Identity”
Ensures the website is who it says it is (and not someone else)
TLS Provides Two Things

“Identity”
Ensures the website is who it says it is (and not someone else)

“Security”
Ensures that only you and the website can read your messages
Identity
You

???

Amazon
You

Trusted Party
(Ex: VeriSign)

???

Amazon
Trusted Party
(Ex: VeriSign)

Private Key

• Kept completely private
• Required to sign a certificate
Trusted Party
(Ex: VeriSign)

Private Key
• Kept completely private
• Required to sign a certificate

Public Key
• Known by everyone
• Can be used to validate that a signature is authentic
Trusted Party
(Ex: VeriSign)

verifies the identity of Amazon

Amazon
A Trusted Party (Ex: VeriSign) signs with a private key to verify the identity of Amazon.
You

???

Trusted Party
(Ex: VeriSign)

Amazon
You

Trusted Party
(Ex: VeriSign)

signed

Amazon

???
You verified with public key Trusted Party (Ex: VeriSign) signed

???

signed

Amazon
You → verified with public key → Trusted Party (Ex: VeriSign) → signed → Amazon

Amazon
You

Trusted Party (Ex: VeriSign)

Does not have a certificate!

Amazon

Does not have a certificate!
Can evil Amazon claim to be real Amazon?

• Option 1: Convince the trusted party that they are really Amazon
Can evil Amazon claim to be real Amazon?
• Option 1: Convince the trusted party that they are really Amazon
• Option 2: Forge a fake signature
Can evil Amazon claim to be real Amazon?

• Option 1: Convince the trusted party that they are really Amazon
• Option 2: Forge a fake signature
courses.engr.illinois.edu uses a certificate that, as of April 2015, Google feels might be able to be faked.
You 

verified with 
public key 

Trusted Party
(Ex: VeriSign)

You

signed

CS 105

CS 105

forged signature

???
TLS Provides Two Things

“Identity”
Ensures the website is who it says it is (and not someone else)

“Security”
Ensures that only you and the website can read your messages
<table>
<thead>
<tr>
<th>Decimal</th>
<th>Binary</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0000</td>
</tr>
<tr>
<td>1</td>
<td>0001</td>
</tr>
<tr>
<td>2</td>
<td>0010</td>
</tr>
<tr>
<td>3</td>
<td>0011</td>
</tr>
<tr>
<td>4</td>
<td>0100</td>
</tr>
<tr>
<td>5</td>
<td>0101</td>
</tr>
<tr>
<td>6</td>
<td>0110</td>
</tr>
<tr>
<td>7</td>
<td>0111</td>
</tr>
<tr>
<td>8</td>
<td>1000</td>
</tr>
<tr>
<td>9</td>
<td>1001</td>
</tr>
<tr>
<td>a</td>
<td>1010</td>
</tr>
<tr>
<td>b</td>
<td>1011</td>
</tr>
<tr>
<td>c</td>
<td>1100</td>
</tr>
<tr>
<td>d</td>
<td>1101</td>
</tr>
<tr>
<td>e</td>
<td>1110</td>
</tr>
<tr>
<td>f</td>
<td>1111</td>
</tr>
</tbody>
</table>
You

Amazon
You

Amazon
Your secret + Amazon secret = Amazon
You

Your secret

Amazon

Amazon secret

9b 68 6c 11 7e 55 71 82 cd 20 58 78 2d 15 0f 09
5d 04 05 56 ea d2 3b 3b 12 a7 eb fd 23 3a c3 fb
c8 01 98 2b 32 06 72 2c 12 f9 0d ee 1c 01 02 23
40 a5 1a d7 ec 56 02 72 13 38 69 41 05 22 64 8a
4e 43 90 ae 8a df 3b b8 d0 29 9d f7 5b 3e 1f 80
f7 ef 17 50 05 be ff 2f 47 7e 99 26 19 c7 7c b7
6a b4 ac 35 c2 91 fc 2d 26 ad d3 63 76 de 3c 09
6b 8d 94 4c 9b 6a 24 1b 03 8c 3b c3 10 67 65 ca
03 b1 a2 25 3c 1c 2a 90 7e 49 e4 45 67 b2 5a 54
34 97 6e 1b 7b 5f c4 d1 b1 a5 1a d6 a5 67 6e ca
1e 6f b9 85 ff 3c 44 2b cd d6 f8 ea f9 d3 46 de
8f bd dd d9 3e fd 50 81 fb 71 72 b0 62 47 6c 91
bd 6e bd 3f be 54 2f c9 ec 51 16 5e c3 77 4a a3
40 63 3e b6 38 7f 81 a0 50 7f 81 d3 a5 7b 7c 1f
a6 09 9f a1 e9 62 44 d0 f8 83 28 9a ae be 3f 03
51 8c 67 51 f9 5b 3a 68 2c 37 9a b3 1c 49 4f 9b
You + Your secret = Amazon secret

Amazon

You
You

Your secret

+ 

= 

Shared secret

Amazon

CS 105 secret

+ 

= 

Shared secret
XOR

0 ← 0 XOR 0 → 0
0 ← 1 XOR 1 → 1
1 XOR 0 → 1
1 XOR 1 → 0
XOR

0 ← 0 XOR 0

0 ← 1 XOR 1

1 ← 0 XOR 1

1 ← 1 XOR 0
Message: 00101001010
Key: 10101011011
Encrypted: 1
Message: 00101001010
Key: 10101011011
Encrypted: 01
Message: 00101001010
Key: 10101011011

Encrypted: 001
Message: 00101001010
Key: 10101011011
Encrypted: 0001
Message: 00101001010

Key: 10101011011

Encrypted: 10001
Message: 00101001010
Key: 10101011011
Encrypted: 10000010001
Message: 00101001010
Key: 10101011011
Encrypted: 10000010001
Encrypted: 10000010001
Encrypted: 10000010001
Message: 00101001010
Key: 10101011011
Encrypted: 10000010001

Encrypted: 10000010001
Key: 10101011011
Message: 
<table>
<thead>
<tr>
<th>Message</th>
<th>00101001010</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key</td>
<td>10101011011</td>
</tr>
<tr>
<td>Encrypted</td>
<td>10000010001</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Encrypted</th>
<th>10000010001</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key</td>
<td>10101011011</td>
</tr>
<tr>
<td>Message:00101001010</td>
<td>00101001010</td>
</tr>
</tbody>
</table>
Message: 00101001010
Key: 10101011011
Encrypted: 10000010001

Encrypted: 10000010001
Key: 10101011011
Message: 10
Message: 00101001010
Key: 10101011011
Encrypted: 10000010001

Encrypted: 10000010001
Key: 10101011011
Message: 010
<table>
<thead>
<tr>
<th>Message</th>
<th>00101001010</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key</td>
<td>10101011011</td>
</tr>
<tr>
<td>Encrypted</td>
<td>10000010001</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Encrypted</th>
<th>10000010001</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key</td>
<td>10101011011</td>
</tr>
<tr>
<td>Message</td>
<td>1010</td>
</tr>
</tbody>
</table>
Exclusive OR (XOR)

Message: 00101001010
Key: 10101011011
Encrypted: 10000010001

Encrypted: 10000010001
Key: 10101011011
Message: 00101001010
You

+ 

Your secret

= 

Shared secret

Amazon

+ 

Amazon secret

= 

Shared secret

Attacker
You + Your secret = Shared secret
Amazon + Amazon secret = Shared secret

Attacker
You

Your secret + = Shared secret

Amazon

Amazon secret + =

Attacker

Yellow + Blue + Blue = Grey
You

Your secret

Amazon

Amazon secret
You

Attacker

Amazon
You + Attacker = Amazon
Message: 00101001010
Key: 10101011011
Encrypted: 10000010001

Encrypted: 10000010001
Key: 10101011011
Message: 00101001010