Lab 3 Report  
Exploring MACs and Hash Functions

**Your Name Here**

# Task 2: Checking Software Digests

1. In Task 2 you should have shown that the software you downloaded from the website was the same software posted on the website. What does it mean if they do not match? If an attacker could break into the website to replace the software with something malicious, what else would the attacker need to replace to get away with it?

TBD

# Task 3: Exploring the “Avalance Effect”

1. Describe the differences between the two digests of iou.txt when the difference between the two inputs is only one bit.

TBD

1. Describe your experience to find another message that matches the original digest of iou.txt.

TBD

1. Referring to your observations and experiences recorded in worksheet items #2 and #3, how does the avalanche effect make it difficult to find two messages that hash to the same value?

TBD

# Task 4: Exploring Second Pre-Image Resistance

1. The last four hex digits of the SHA256 digest of declare.txt: \_\_\_\_\_\_\_\_\_\_\_\_
2. The number of attempts to match on **the last hex digit** of the digest for declare.txt.

|  |  |
| --- | --- |
| Attempt | # Tries |
| 1 |  |
| 2 |  |
| 3 |  |
| 4 |  |
| 5 |  |
| 6 |  |
| 7 |  |
| 8 |  |
| 9 |  |
| 10 |  |

1. Referring to the data reported in item #6 above, why are the results so different amongst the ten attempts to find a match on the last digit of the digest? If a hex digit only has 16 possible outputs, why would it take more than 16 times to sometimes find a collision?

TBD

1. The number of attempts to match on the last **two** hex digits of the digest for declare.txt.

|  |  |
| --- | --- |
| Attempt | # Tries |
| 1 |  |
| 2 |  |
| 3 |  |
| 4 |  |
| 5 |  |
| 6 |  |
| 7 |  |
| 8 |  |
| 9 |  |
| 10 |  |

1. The number of attempts to match on the last **three** hex digits of the digest for declare.txt.

|  |  |
| --- | --- |
| Attempt | # Tries |
| 1 |  |
| 2 |  |
| 3 |  |
| 4 |  |
| 5 |  |
| 6 |  |
| 7 |  |
| 8 |  |
| 9 |  |
| 10 |  |

1. Referring to the graph in the Excel spreadsheet, what kind of pattern do you see in the graph? What does this suggest if you tried to find a match against the entire hash for declare.txt?

TBD

# Task 5: Exploring Collison Resistance

1. The number of attempts to find two random messages whose digests match on the last byte (i.e., the last **two** hex digits).

|  |  |
| --- | --- |
| Attempt | # Tries |
| 1 |  |
| 2 |  |
| 3 |  |
| 4 |  |
| 5 |  |
| 6 |  |
| 7 |  |
| 8 |  |
| 9 |  |
| 10 |  |

1. Referring to the tables in items #8 and #11, when only two hex digits needed to match, explain why it required less effort to find a collision in #11 than it did in #8.

TBD

# Task 6: Exploring Message Authentication Codes

1. Describe your observations about the differences in the outputs when different keys are used to generate an HMAC for the same file.

TBD

1. At the end of Task 6 you found a MAC key through a “brute force” effort. What could an adversary do if he could determine the MAC key that is used to protect the integrity of communications between two people?

TBD

# Other

1. Describe any experimentation that you performed.

TBD

1. What did you learn from this exercise?

TBD

1. How could this lab exercise be improved?

TBD