**Lab Practice 01**

**Hash**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Matrícula | **A01366288** | Name | **Alan Macedo Esparza** | Group | **4** | Date | **8/12/20** |

**Write the requested answers on this document. Create a PDF file and upload it to Canvas**

1. Research  
   Investigate the concepts and write a description of each one.

|  |  |
| --- | --- |
| Concept of Hash | A transformation of data, that maps arbitrary-sized data onto a fixed size. Often used for hash-maps and similar data structures. |
| MD5 | MD5 is a hash function that maps inputs onto a 128-bit hash value. |
| MD4 | MD4 is a predecessor to MD5. MD stands for message-direct. As with MD5, it maps inputs onto 128-bit values. |
| SHA1 | Similar to MD5, SHA-1 maps inputs onto 160-bit values. It was developed by the NSA. |
| SHA256 | SHA 256 belongs to the SHA-2 family, also designed/developed by the NSA. It has a 32-bit word size. It has a 256-bit output. |
| SHA384 | SHA384 belongs to the SHA-3 family, it has a 384-bit output. It has 192-bit security. |
| SHA512 | As with SHA-256, SHA512 also belongs to the SHA-2 Family of functions. It has 256-bit security, and has a 512-bit output |
| RIPEMD-160 | A strengthened version of RIPEMD, it outputs a 16-byte result. |
| PANAMA | can be used both as a hash function and a stream cipher. 256 bits block size. |
| TIGER | The size of a Tiger hash value is 192 bits. |

1. Install the program HashCalc 2.02, called HashCalc.exe (Requires Windows)

<https://www.slavasoft.com/hashcalc/>



1. Run the program HashCalc.exe

In the Data Format combo select: Text String.

In the Data field write: Hello World



1. Press the Calculate button (below) and write the results.

In the second column write or paste the results given by the program.

In the third column deduce or write the value of the bits used according to your research on subsection 1

In the fourth column calculate the number of bytes of column 3 or count the bytes of the result (remember that one byte is formed by two nibbles o hexadecimal digits).



Calculate all the results (\*)

(\*) Compare results with your classmates

|  |  |  |  |
| --- | --- | --- | --- |
| **Function** | **Data on Hexadecimal** | **Number of bits** | **Number of bytes** |
| MD5 |  |  |  |
| MD4 |  |  |  |
| SHA1 |  |  |  |
| SHA256 |  |  |  |
| SHA384 |  |  |  |
| SHA512 |  |  |  |
| RIPEMD-160 |  |  |  |
| PANAMA |  |  |  |
| TIGER |  |  |  |

1. Repeat the process with Hello World. (add one point at the end)

Fill the same table the new values (add a new line for each function)

What did you notice on the table?

|  |
| --- |
|  |

1. Create a text file on Notepad which contains ONLY Hello World (no spaces, no ENTER)

Save it with tha name HelloWorld.txt

Now open it as File on the Data Format combo.

Fill the same table again with the values calculated on a third line.



1. Investigate what HMAC is.

|  |  |
| --- | --- |
| HMAC Concept |  |

1. Repeat the process with Hello World

Data Format: Text String

Data: Hello World

Check box HMAC (selected)

Key Format: Text string

Key: CyberSec

Fill the table with the results on a forth line.

What did you notices on the table?

|  |
| --- |
|  |

1. If you create a program file.

How would you use this to make sure the program file is not modified or affected by a malware? Discuss this with your classmates.

|  |
| --- |
|  |

Write a reflection aboud this lab in at least 5 lines. (what you thought before, during and after this lab practice).

|  |
| --- |
|  |

What do you expect to learn this semester with the Computer and Security Labs?

|  |
| --- |
|  |