|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | **Hope Foundation’s,**  **Finolex Academy of Management and Technology, Ratnagiri** | | | | | | | | | |
| **Department of Information Technology** | | | | | | | | | |
| Subject name: SECURITY LAB | | | | | | | | Subject Code: ITL502 | | | |
| Class | | TE IT | | Semester – V (CBCGS) | | | | Academic year: 2018-19 | | | |
| Name of Student | | Kazi Jawwad A Rahim | | | | | **QUIZ Score :** | | | | |
| Roll No | | 32 | | | Experiment No. | | | | | 04 | |
| Title**. To Test integrity of message using MD-5, SHA-1, and analyze the performance of the two protocols using crypt APIs.** | | | | | | | | | | | |
|  | | | | | | | | | | | |
| 1. **Course objectives applicable:**   **LOB3**. To analyze and evaluate performance of hashing algorithms | | | | | | | | | | | |
| 1. **Course outcomes applicable:**   **LO3.**  Analyze and evaluate performance of hashing algorithms | | | | | | | | | | | |
| **3. Learning Objectives:**   * To analyze and evaluate performance of hashing algorithms | | | | | | | | | | | |
| **Practical applications of the assignment/experiment:**   * This algorithm is suitable to calculate hash for small chunks of in-memory string data. * To process large external files (like ISO images) you should use MessageDigest class directly * There may be difficulties while processing string data in encodings other than iso-8859-1. | | | | | | | | | | | |
| **Prerequisites**:  In cryptography, hash function generates a unique value for a given data. | | | | | | | | | | | |
| **6. Hardware Requirements**:   1. PC with 4GB RAM, 500GB HDD.   **7. Software Requirements:**  1. Programming language C, C++, Java, Python | | | | | | | | | | | |
|  | | | | | | | | | | | |
| **8. Quiz Questions (if any): (Online Exam will be taken separately batchwise, attach the certificate/ Marks obtained)**   1. What are MD4 and SHA? 2. Describe some characteristics of MD5 and SHA. 3. Why MD5 is not secure to store passwords? 4. Define Hash collision. 5. Secure Hash function or algorithm was developed by whom? | | | | | | | | | | | |
|  | | | | | | | | | | | |
| **9. Experiment/Assignment Evaluation:** | | | | | | | | | | | |
| **Sr. No.** | **Parameters** | | | | | | | | **Marks obtained** | | **Out of** |
| **1** | Technical Understanding (Assessment may be done based on Q & A **or** any other relevant method.) Teacher should mention the other method used - | | | | | | | |  | | 6 |
| **2** | Neatness/presentation | | | | | | | |  | | 2 |
| **3** | Punctuality | | | | | | | |  | | 2 |
| **Date of performance (DOP)** | | |  | | | **Total marks obtained** | | |  | | **10** |
| **Date of checking (DOC)** | | |  | | | **Signature of teacher** | | | | | |

**Result:**

**Source Code: MD5**

import hashlib

str="1234567890"

result=hashlib.md5(str.encode())

print(result.hexdigest())

**Source Code: SHA**

import hashlib

str="1234567890"

result=hashlib.sha1(str.encode())

print(result.hexdigest())

**OUTPUT**

|  |  |  |
| --- | --- | --- |
| **Test Strings** | **MD5 VALUE** | **SHA VALUE** |
| THIS IS SECURITY LAB PROGRAM FOR MD5 | **0deac9137a3d5a30198ebcd6cc797b62** | **af47f3a9f7861e658f5acc5a8fba6cda8497df48** |
| THIS IS SECURITY LAB PROGRAM FOR SHA | **0deac9137a3d5a30198ebcd6cc797b62** | **fdf3ea8d464fe4d2c257dbbb811075d92b250440** |
| NULL STRING “” | **d41d8cd98f00b204e9800998ecf8427e** | **da39a3ee5e6b4b0d3255bfef95601890afd80709** |
| 1234567890 | e807f1fcf82d132f9bb018ca6738a19f | 01b307acba4f54f55aafc33bb06bbbf6ca803e9a |
| abcdefghijklmnopqrstuvwxyz | c3fcd3d76192e4007dfb496cca67e13b | 32d10c7b8cf96570ca04ce37f2a19d84240d3a89 |
| abcdefghijklmnopqrstuvwxyz1234567890 | 7f7d52a001b9d2c71b6bae1f189f41f3 | dea3c171abcdfb3e8380d6860630f618eb6e074f |
| ABCDEFGHIJKLMNOPQRSTUVWXYZ | 437bba8e0bf58337674f4539e75186ac | 80256f39a9d308650ac90d9be9a72a9562454574 |
| message digest value is | 4e78a08533c3e349490e698c421f76c7 | 0e7d427e88f7c945055f0ae581301023181aa1a7 |
| @IamJRKOO6 | 4eca64167d848bd5c38fedf6df0d75cd | c31f68a8f10f3b5d62a4f05938bce7325c1ecdfb |

**Differences between MD5 and SHA Algorithms**

****

**Similarities between MD5 and SHA Algorithms**

**References** :

[1] Rivest R., 1992, “The MD5 Message-Digest Algorithm,”RFC 1321, MIT LCS and RSA Data Securit y, Inc.

[2] Kahate, Atul, 2003, "Cryptography and Network Securit y", Tata McGraw-Hill ,India.

[3] Kasgar A. K., Agrawal Jitendra, Sahu Santosh, 2012, “New Modified 256-bit MD5 Algorithm with SHA Comp