UNIVERSITY OF COLOMBO SCHOOL OF COMPUTING

IS2109 Information Systems Security - Practical 9

Cryptography

Instructions:

- **Submit answers for all the following questions. Clearly mention the Question Numbers.**
- **You must submit your answers as a PDF document named as P9_IndexNumber (E.g. P9_17000000)**

Note :

Windows PowerShell

1. **Generate MD5 and SHA-1 checksum of a file**

   ```
   Get-FileHash File Path -Algorithm MD5

   Get-FileHash File Path -Algorithm SHA1
   ```

2. **Check integrity of a directory containing files(Using MD5)**

   ```
   Get-ChildItem | Get-FileHash -Algorithm MD5
   ```

Linux

1. **Generate MD5 and SHA-1 checksum of a file**

   ```
   $ md5sum filename

   $ sha1sum filename
   ```

2. **Check integrity of a directory containing files (Using MD5)**

   ```
   $ md5sum * > ../integritymd5

   $ cat ../integritymd5
   ```

**** Provide screenshots where necessary, for the following questions****

Checking integrity

1. Generate the MD5 and SHA-1 hash values for the attached 'Text1.txt' file
2. Try to check the integrity of the files in the provided folder/directory
3. Change something in one of the files and check whether you can catch the changed file.

Collisions in MD5 and SHA-1

1. Checkout the MD5 hash values of attached two images.
2. When you are downloading a software from the internet, you might have noticed that the hash value of the setup file is displayed on the downloading page.

   Ex: Netbeans download page.

   Explain the reason behind that.
3. Researchers have recently found out about a SHA1 collision. Read about their works and calculate hash values of the sample PDF files on the website. https://shattered.io/

Reverse Hashing

1. When you forget a password of a standard website, they ask you to create a new password rather than just sending your forgotten password . Explain why?
2. Calculate the MD5 hash value of the text "hello". Google that hash value and examine the results.
3. Create a SHA1 hash of your name, X=Hash(NAME) by using a command line tool. Try X on SHA1 reverse lookup web site.
4. If these hashing algorithms are one-way functions, how is it possible to have these reversed hashes available on the web. Explain the reverse hashing procedure used by those lookup sites.
5. Explain how passwords(which has been stored as hashes), can be protected from reverse hashing