Information Security
Assignment 3

Group 31
Stijn Kammer (s4986296) & Ramon Kits (s5440769)

October 10, 2022

Exersize 1

Code to be found at Themis.

Exersize 2

Code to be found at Themis.

Exersize 3

SHA-256 is a hashing algorithm which produces 256 bit hashes based on its input. That means a hash would have 2^{256} possibilities. To have a 100% chance of finding a collision, you would need to try $2^{256} + 1$ hashes. That equates to over 10^{77} hashes in decimal notation, over 200 million times the amount of atoms in the Milky Way galaxy. As of the time of writing, which is October 2022, the world's population is 7.98 billion. If every person on earth would write a document once a day and sign it with SHA-256, it would take $\frac{10^{77}}{7.98 \times 10^{12}}$ days to definitely find a collision. That still leaves us with 1.25×10^{64} days, which is 3.43×10^{61} years.

Exersize 4

Checksums make the risk of running malicious code smaller. As long as you can trust the checksum of the file, it should be safe to run. HTTP sends data using plain text, which means it is vulnerable to content spoofing attacks. Secure HTTP (HTTPS) does not do this, as it uses SSL/TLS to encrypt the data. And provide a certificate to verify the identity of the server.

If a user enters a webiste that uses HTTPS, the browser can check the certificate and thus make sure that the website is the one it claims to be and thath the checksums can be trusted. If the user enters a website that uses HTTP, the browser can't check the certificate and thus can't make sure that the website is the one it claims to be. Attackers might use this to serve malicious code to the user. If the user downloads a file from the website, the checksum can't be trusted and the user might run that malicious code.

When redirecting a user from HTTP to HTTPS, you prevent the user from getting served tempered content. This makes it less likely for the user to see an edited version of the checksum. Also, when the user gets redirected from HTTP to HTTPS, the data security is still preserved for downloading files and viewing the checksums, since before the redirect, the user does not download any files and the checksums are not yet shown. When merely using HTTP, the user can be served tempered content, which means the user can be shown a different checksum than the one that is actually used to verify the file. This way, the user can be tricked into running malicious code.

Exersize 5

A hidden message has been placed in the first hashing slide of the lecture. After a close examination of the slide, it can be found that the message is:

> "secretwriting"

This message was hidden in the text of the slide. Because of the wording in the text it was apparent that it should contain a secret message. The message was hidden by making a text that had for every word the third character in common with the next character of the word in the message as follows:

> "Ye**S**, th**E** al**C**hemists wo**R**shipped th**E** an**T**imatter, vo**W**ing da**R**k, ag**I**le ac**T**ions wh**I**le an**N**ouncing al**G**ebra..."

Work distribution

The work was distributed rather evenly between the two students. Ramon initially wrote the code for exersize 1, while Stijn wrote the code for exersize 2. Later on Ramon helped Stijn with exersize 2 because of the complexity of the code. Both students worked on the answers for exersize 3, 4 and 5.