Desmond Hughes

Purdue University Global

IT262 Certified Ethical Hacking I

Cheryl Waters

September 3, 2022

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text

Description automatically generatedGraphical user interface, text, application

Description automatically generatedGraphical user interface, text

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text

Description automatically generated

Graphical user interface, text

Description automatically generated

Graphical user interface, text

Description automatically generated

Graphical user interface, text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Graphical user interface, text

Description automatically generated

Graphical user interface, text, application

Description automatically generatedGraphical user interface, text

Description automatically generated

Part 2: A cryptographic Hash is a hash function that is used for security purposes. Cryptographic Hash is used when you need security and privacy. It is also slower than all of the other hashes. There are multiple function properties requirements of this hash, One is speed, which means the cryptographic hash should be working efficiently. Another property it needs to have been the avalanche effect, which is shows if any data has been offered. Cryptographic hash should also be deterministic, this means no matter how many times you enter the same input you will always get the same output. Another property it must have been pre-image resistance, which means that is hard to get to get to the input with the output. The last property is collision resistance, which means different messages or inputs should not be able to produce the same output or hash value.

To exchange a message using public key cryptography with already generated keys you will first need to export your public key. Then you will need to exchange public keys with the person you want to send a message to. Import the person you want to send the message to key, and after that verify the keys so that you know that you are using the right ones. Encrypt the message you want to send, and then you can send it. When you’ve received it, you can decrypt it with the private key. Then you would sign a message to verify the data wasn’t messed with.

Reference

(2020). Retrieved 6 September 2022, from https://howchoo.com/security/how-to-send-and-receive-encrypted-messages-using-gpg

Georgiev, D. (2022). What Is Cryptographic Hash? [A Beginner’s Guide]. Retrieved 6 September 2022, from https://techjury.net/blog/what-is-cryptographic-hash/#gref