En bild som visar Teckensnitt, text, vit, Grafik

Automatiskt genererad beskrivning

Linnaeus University

1DV700 - Computer Security

Assignment 1

Student: Ebbe Karlstad

Personal number: 041025–5434

Student ID: ek224ev@student.lnu.se

En bild som visar skiss, växt, rita, botanik

Automatiskt genererad beskrivning

Setup Premises

Explain your setup such as, OS, web browser, tools being used, development environment, and whatever else is necessary…

Task 1

a) Symmetric encryption is a form of encryption where plain text, or whatever is supposed to be encrypted does so with a key, and when that encrypted message is to be decrypted, it does so with the same key. Since the encryption and decryption key is the same, it is easy to do but less secure and requires a safe way to transfer the key between parties. Asymmetric encryption is a form of encryption where the encrypted message gets encrypted with a public key, and then gets decrypted with a private key, where the public and private keys are different. This process is slower, but also more secure [1].

Encryption and Hashing algorithms are a bit different. When you encrypt something, you scramble the message you want to encrypt, with a key, which will result in a ciphertext. This means that with that key you can also decrypt it, returning it into plain text. Encryption is a two-way process. Hashing on the other hand, converts information using a hash function, and returns a hash key, which cannot be reverted, hence it is a one-way process. Examples of encryption algorithms are RSA and AES, and examples of hashing algorithms are MD5 and SHA256 [2].

Hashing, as mentioned before, is the process of converting information using a hashing algorithm, or a hash function, to create a hash key. Compressing information works a bit differently, by encoding information using fewer bits than the original message. A device that does compression is usually referred to as an encoder, and a device that decompresses information is called a decoder [3].

b) Steganography is often described as hiding something in plain sight. This is usually done by embedding digital information in standard files, this could be embedding code with a message in it into an image file and sending that in an email to the person the message is for [4].

Digital watermarking is very similar to steganography, with one deviation, in digital watermarking, if a message is embedded and hidden inside an image, the message can be either hidden or visible, in steganography, the message is always hidden. [5]

The biggest difference between encryption and steganography/digital watermarking is that encryption hides the message, but not the existence of it, while both steganography and digital watermarking hides the existence of the message itself.

Task 2

a) For this simple substitution cipher, we have the encrypted message: “HKPUFCMHY BHDDXZH” and we want to decrypt it using the table provided in the question. To do this, we simply look at the table and replace the ciphered letters with the corresponding plain text letters, so H becomes e, k becomes n and so on. The final decrypted message is: “encryption message”.

b) For the other simple substitution cipher, we have the encrypted message: “NWSRC XQS JXB CWRGABY WKH VWUNWBA” and we want to decrypt it without knowing the key. When I saw this question, I immediately thought of the monoalphabetic cipher, which is simply replacing a letter in the plain text message with another letter to get the ciphered text. Note that the letters used to encrypt this message usually does not have any relation to each other, which makes it harder to crack. The way to approach these ciphers is to use the frequency of the most used letters in the encrypted text and replace them with the most frequently used letters in the English language.

Bibliography

|  |  |
| --- | --- |
| [1] | gluttony777, ”GeeksForGeeks,” 22 May 2023. [Online]. Available:  https://www.geeksforgeeks.org/difference-between-symmetric-and-asymmetric-key-encryption/.  [Använd 13 November 2023]. |
| [2] | CoderSaty, ”GeeksForGeeks,” 7 May 2023. [Online]. Available:  https://geeksforgeeks.org/difference-between-hashing-and-encryption/.  [Använd 13 November 2023]. |
| [3] | S. -J. Behrens, ”JavaCodeGeeks,” 26 September 2020. [Online]. Available:  https://www.javacodegeeks.com/2020/09/hashing-encryption-encoding-compression-oh-my.html.  [Använd 13 November 2023]. |
| [4] | ”How does steganography work and does it threaten enterprise data?,” 13 January 2014. [Online].  Available: https://moodle.lnu.se/pluginfile.php/8283582/mod\_resource/content/1/  How%20does%20steganography%20work%20and%20does%20it%20threaten%  20enterprise%20data%3F.pdf. [Använd 13 November 2023]. |
| [5] | C. Brook, ”Digital Guardian,” [Online]. Available: https://www.digitalguardian.com/blog/digital-watermarking.  [Använd 13 November 2023]. |