Security and Cryptography Lab 6

Introduction.

Steganography – the science of communication in such a way that the presence of a message cannot be detected. Unlike cryptography (where the presence of a message is not negated, but its content is implicit), steganography attempts to conceal the fact that communication is taking place.

Steganographic techniques are also used to tag digital data. Steganographic systems can be divided into:

- pure steganography – the strength of the technique is based on the attacker's ignorance of the method. These systems do not meet the Kerckhoffs principle, so they are not recommended.
- private key steganography – the method is open and widely available, before the communication begins, the parties take into account the steganographic key used in a method-dependent manner, but there is a problem with handing over the key in a secure way.
- public key steganography – similar to asymmetric cryptographic systems, two keys are used – public and private. The public (explicit) key is used to embed the message in the carrier, while the private key is used to extract it.

Password cracking – In cryptanalysis and computer security, password cracking is the process of recovering passwords from data that has been stored in or transmitted by a computer system in an encrypted form. A common approach (brute-force attack) involves repeatedly trying to guess the password and checking it against the available cryptographic hash of the password. Another type of approach is password spraying using a list of common passwords, which is often automated and occurs slowly over /me to remain undetected.

Task 1.

Hiding data with steganography techniques

1. Create a folder on your disk called *Task1* and a subfolder called *Original*.
2. Download 4 sample images from the Internet in *jpg* format and place them in the *Original* folder.
3. In the *Original* folder, create four files in *txt, docx, xlsx* and *zip* formats with any content.
4. Place the newly created *txt, docx, xlsx, zip* files and the text message '*HIDDEN MASSAGE: YourNameAndSurname*' in each jpg file separately using any method.
5. Save the newly created jpg files to a new folder named *Hidden*.

Zip folder Task1 and attach the files to the resulting file.

6. Answer the following questions:
   1. Describe how you hide sample files and message.
   2. Describe how we can retrieve hidden files and message from an image.
   3. Suggest some method to detect the fact that files are hidden.
   4. Is there any differences between hiding a file or folder in an image?

Task 2.

1. With the help of the 7z software, create three archives with any files. When creating, encrypt the archives using the following passwords and crypt method AES-256 (save this files in *Task2* folder):
   - archive_01.zip – password: 12345
   - archive_02.zip – password: password0
   - archive_03.zip – password: abcde
   - archive_04.zip – password: no1
2. Check using sources from previous labs or find new methods online:
   - the strength of the above passwords,
   - how any possible combinations should you consider when brute force password cracking?

Response

3. Use **John the Ripper** and crack all of the above passwords. Make a note of the times the password was guessed.

Screenshots + Description

4. Use the **Hashcat** program and crack all the above passwords.

Screenshots + Description

5. Answer the following questions:
   1. Were all the passwords recognized using **John the Ripper** and **Hashcat**? If no, why?
   2. Suggest and execute a method to reduce the time it takes to crack a password.

Summary and submission of exercise results:

1. Create one PDF file called ***results-yoursFirstName_yoursLastName_yyyy_mm_dd.pdf***. By putting in it:
   1. answers to all questions included in pdf files from three exercises,
   2. answers to all my questions.
2. Create one ZIP file called *results-yoursFirstName_yoursLastName_yyyy_mm_dd.zip*.
3. In the ZIP file, you put the resulting files from the tasks.
4. Ready-made PDF and ZIP files are placed on the e-learning website.

yyyy_mm_dd – this is the date of the class, i.e. the class from 06.03.2025, it will be, for example, a file named *results-yoursFirstName_yoursLastName_2025_03_06.*zip. **Misspelled names will be removed and the exercise will be failed.**

Evaluate:

1. Work submitted on time - grade range 5 - 2.
2. Work submitted 7 days after the deadline - grade range 4.5 - 2.
3. Work submitted 7-14 days after the due date - grade range 4 - 2.
4. Work submitted 14-30 days after the due date - grade range 3 - 2.

For example, the task of 06.03.2025 submitted by 12.03.2025 at 6 p.m. will be assessed in accordance to point 1