

## Lab: Cryptanalysis Attack

### Cryptanalysis Attack

#### Introduction

This lab introduces you to cryptanalysis using the CrypTool 2.1 software. You will explore the process of breaking Data Encryption Standard (DES) encryption through known plaintext/Ciphertext Only attack. By following step-by-step instructions, you will observe how cryptanalysis techniques are used to derive the deciphered text and the encryption key, understanding the underlying vulnerabilities of symmetric encryption algorithms like DES.

#### Learning objectives

After completing this lab, you will be able to:

- Perform a known plaintext/Ciphertext Only attack on the DES encryption algorithm
- Analyze how to recover a deciphered message and key using cryptanalysis techniques
- Observe the vulnerabilities in symmetric encryption methods like DES

---

### Part 1: Installing CrypTool 2.1

*Note: If you have CrypTools already installed, you can skip to Part 2: DES Cryptanalysis.*

#### Step 1: Download CrypTool 2.1

- **CrypTool 2.1** is the current version available as a desktop application.
- Go to the official CrypTool website: <https://www.cryptool.org/en>.  
(**Note:** To open the links, right-click (or long-press) on the links and select "Open in new tab." Avoid clicking the link directly, as this might block it.)


#### Step 2: Install CrypTool 2.1 on Windows

- Download **CrypTool 2.1 (Stable Build 9778.2)** from the official website:
  - Go to [CrypTool 2 Download Page](#).\*(**Note:** To open the links, right-click (or long-press) on the links and select "Open in new tab." Avoid clicking the link directly, as this might block it.)

- Select the version compatible with your operating system (typically a .exe file for Windows).
- Run the installer by double-clicking the downloaded file.
  - Follow the prompts and accept the default installation options.

## Part 2: Performing DES Cryptanalysis

- Open **CrypTool 2.1**.
- Select **New** option.
- Select **Cryptanalysis** and click on **Next**.
- Select **Modern Encryption** and click on **Next**.
- Select **Symmetric Encryption** and click on **Next**.
- Select **DES** and click on **Next**.
- Select **Known Plaintext** and click on **Next**.
- Keep all the default values unchanged and select **Next**.
- Observe the Cryptanalysis process. It will generate **Deciphered Ciphertext** and a **Key** based on analysis. The generated output may be partially or fully correct.


**WIZARD**

AES KNOWN-PLAINTEXT ANALYSIS OUTPUT

Here, you can see the DES analysis.

Analyzer:

| Local   |   | Start:                  | 8/11/2025 2:01 PM             | Estimated end:                | 8/11/2025 2:01 PM |
|---------|---|-------------------------|-------------------------------|-------------------------------|-------------------|
|         |   | Elapsed time:           | 4 seconds                     | Remaining time:               |                   |
|         |   | Bits to be tested:      | 24                            | Keys / sec:                   | 3,647,679         |
| Top Ten | # | Value                   | Key                           | Text                          |                   |
|         | 1 | 1                       | A1-B1-C1-11-11-10-10-10       | Hallo Welt, das ist ein Test  |                   |
|         | 2 | 1                       | A1-B1-C1-11-11-10-10-11       | Hallo Welt, das ist ein Test  |                   |
|         | 3 | 1                       | A1-B1-C1-11-11-10-11-10       | Hallo Welt, das ist ein Test  |                   |
|         | 4 | 1                       | A1-B1-C1-11-11-10-11-11       | Hallo Welt, das ist ein Test  |                   |
|         | 5 | 1                       | A1-B1-C1-11-11-11-10-10       | Hallo Welt, das ist ein Test  |                   |
|         | 6 | 1                       | A1-B1-C1-11-11-11-10-11       | Hallo Welt, das ist ein Test  |                   |
|         | 7 | 1                       | A1-B1-C1-11-11-11-11-10       | Hallo Welt, das ist ein Test  |                   |
|         | 8 | 1                       | A1-B1-C1-11-11-11-11-11       | Hallo Welt, das ist ein Test  |                   |
|         | 9 | 0                       | A1-B1-C1-11-11-00-00-00       | "o?ucavüdBİ=a\ "%/fEpi'.Ä9M"± |                   |
| 10      | 0 | A1-B1-C1-11-11-00-00-01 | "o?ucavüdBİ=a\ "%/fEpi'.Ä9M"± |                               |                   |

---

## Exercise

- Perform the DES Cryptanalysis using "**Ciphertext Only**" and observe the output.

here, you can see the DES analysis.

Analyzer:

| Local | Start:             | 8/11/2025 2:02 PM | Estimated end:  | 8/11/2025 2:03 PM |
|-------|--------------------|-------------------|-----------------|-------------------|
|       | Elapsed time:      | 9 seconds         | Remaining time: | 42 seconds        |
|       | Bits to be tested: | 24                | Keys / sec:     | 327,423           |

|         | #  | Value | Key                     | Text                              |
|---------|----|-------|-------------------------|-----------------------------------|
| Top Ten | 1  | 4.72  | A1-B1-C1-11-11-10-10-10 | Der Data Encryption Standard (DE. |
|         | 2  | 4.72  | A1-B1-C1-11-11-10-10-11 | Der Data Encryption Standard (DE. |
|         | 3  | 4.72  | A1-B1-C1-11-11-10-11-10 | Der Data Encryption Standard (DE. |
|         | 4  | 4.72  | A1-B1-C1-11-11-10-11-11 | Der Data Encryption Standard (DE. |
|         | 5  | 4.72  | A1-B1-C1-11-11-11-10-10 | Der Data Encryption Standard (DE. |
|         | 6  | 4.72  | A1-B1-C1-11-11-11-10-11 | Der Data Encryption Standard (DE. |
|         | 7  | 4.72  | A1-B1-C1-11-11-11-11-10 | Der Data Encryption Standard (DE. |
|         | 8  | 4.72  | A1-B1-C1-11-11-11-11-11 | Der Data Encryption Standard (DE. |
|         | 9  | 6.898 | A1-B1-C1-11-11-1A-D6-AC | ,use"tbe"8 7>EeSÅW0"Ebdc....      |
|         | 10 | 6.898 | A1-B1-C1-11-11-1A-D6-AD | ,use"tbe"8 7>EeSÅW0"Ebdc....      |

Progress:

---

## Summary

In this reading, you used CrypTool 2.1 to perform a cryptanalysis of DES encryption through a known plaintext/Ciphertext Only attack. The process involved selecting the DES algorithm and analyzing encrypted text to recover the deciphered message and key. This exercise provided insights into the weaknesses of symmetric encryption, demonstrated how known plaintext attacks work, and displayed the ability of cryptanalysis tools to decrypt messages without knowing the original key.

### My summary

In this optional lab, I used **CrypTool 2.1** to perform a cryptanalysis of **DES (Data Encryption Standard)** using both **Known Plaintext** and **Ciphertext-Only** attacks.

- In the **Known Plaintext attack**, CrypTool successfully analyzed the encrypted data by matching the provided plaintext against possible key candidates, returning a partially or fully correct deciphered message and key.
- In the **Ciphertext-Only attack**, CrypTool attempted to decrypt the message without any knowledge of the original plaintext. The results demonstrated the limitations of

such an attack, showing that the deciphered output may be only partially readable or not entirely accurate.

This lab reinforced the concept of **symmetric encryption vulnerabilities** and how cryptanalysis tools can exploit weaknesses like predictable input or low key complexity in older algorithms like DES.