Krypton

Level 0 – 1

Step 1: Accessing the Krypton Wargame Portal

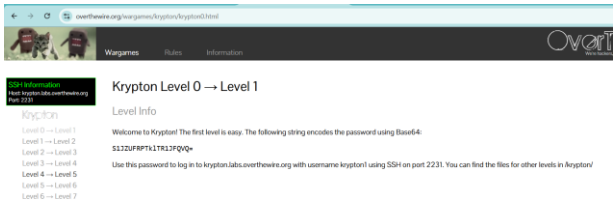
- **Tool Used:** Web Browser
- **Action Taken:**
  Opened the URL: https://overthewire.org/wargames/krypton/

Explanation:

- This URL points to the official OverTheWire Krypton wargame portal.
- It provides:
  - Introduction to the Krypton series.
  - Instructions on how to start Level 0.
  - SSH login details including username and port.

Purpose:

- To understand the challenge and prepare for logging into Level 0.



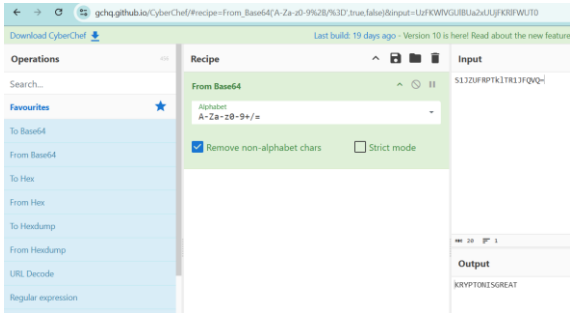
Step 2: Decoding the Password Using CyberChef

- **Tool Used:** CyberChef (Online Tool)
- **Action Taken:**
  Used the "From Base64" operation in CyberChef.
- **Explanation:**
  - The Level 0 challenge presented a string that was Base64 encoded.
  - Base64 is a common encoding method that converts binary data into ASCII text.
  - In CyberChef:
    - Pasted the encoded string.
    - Selected the "From Base64" operation.

- Successfully decoded the string to reveal the **plaintext password** for Level 1.

Purpose:

- To obtain the login password for connecting to Krypton1.



Step 3: SSH Login into Krypton1 Using Kali Linux

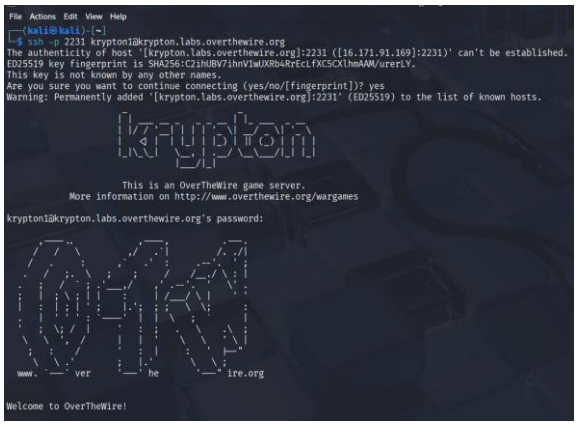
- **Tool Used:** Kali Linux Terminal (SSH Client)
- **Command Executed: ssh -p 2231 krypton1@krypton.labs.overthewire.org**

Explanation:

- Used the decoded password from CyberChef to log in.
- Connected to the remote server over port `2231` using SSH.
- Logged into the `krypton1` account to begin Level 1.

Purpose:

- To access the Krypton1 server and proceed with the next level of the wargame.



Level 1 → Level 2

Step 1: Accessing Level 1 Instructions in Browser

- **Tool Used:** Web Browser
- **Action Taken:**
  Opened the URLs:
  https://overthewire.org/wargames/krypton/krypton1.html

Explanation:

- These pages contained:
  - Specific guidance for solving **Level 1**.
  - Details about the type of encryption used in the challenge.
- The information hinted that the text was encoded using a **simple cipher**.

Purpose:

- To understand the context of the encryption method used in Level 1 and gather hints before proceeding.

Step 2: Exploring Files on the Krypton1 Server

- **Tool Used:** Kali Linux Terminal
- **Commands Executed:** cd /krypton/krypton1

  : ls

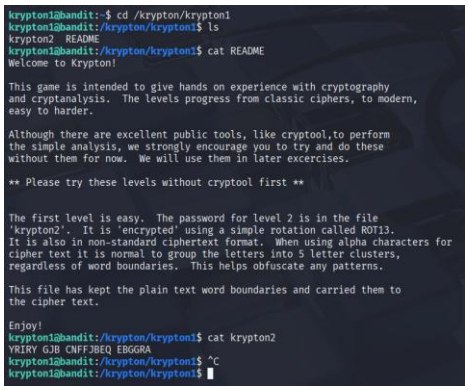
  : cat README
  : cat krypton2

Explanation:

- Navigated to the /krypton/krypton1 directory where challenge files were stored.
- Listed available files using ls.
- Read the README file, which provided hints about the encryption type.
- Displayed the contents of the krypton2 file, which contained the **encrypted text** needed to solve the level.

Observation:

- The encryption used was identified as **ROT13** based on the README hints.

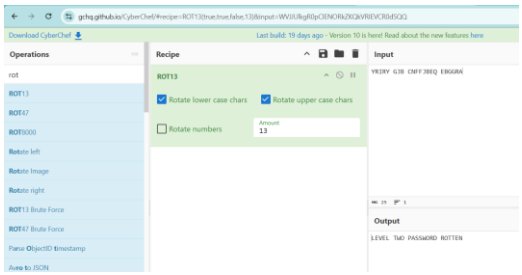


Step 3: Decoding the Encrypted Text Using CyberChef

- **Tool Used:** CyberChef (Online Tool)
- **Action Taken:**
  Applied the "ROT13" operation on the encrypted text.
- **Explanation:**
  - **ROT13** (Rotate by 13 places) is a simple letter substitution cipher.
  - In CyberChef:
    - Pasted the ciphertext from krypton2.
    - Selected the "ROT13" operation.
    - Successfully decoded the text to reveal the password for **Krypton2**.

Purpose:

- To obtain the next level's password by decoding the ROT13 ciphered text.



Level 2 → Level 3

Step 1: Accessing Level 2 Instructions in Browser

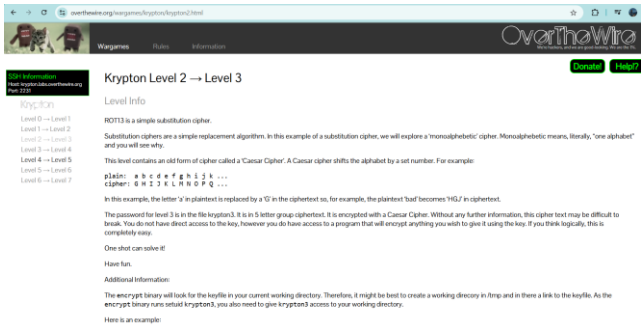
- **Tool Used:** Web Browser
- **Action Taken:**
  Opened the URL =
  https://overthewire.org/wargames/krypton/krypton2.html

Explanation:

- This page provided:
  - Hints related to the encryption method used in Level 2.
  - Instructions suggesting that some binary encryption mechanism might be involved.

Purpose:

- To understand the encryption challenge setup for Level 2.

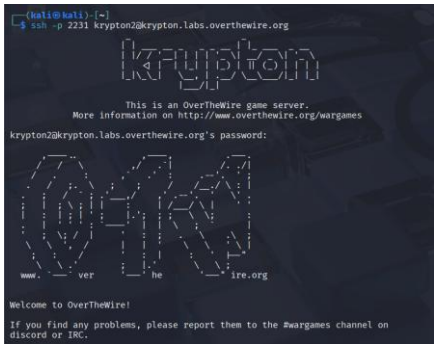


Step 2: SSH Login into Krypton2

- **Tool Used:** Kali Linux Terminal (SSH Client)
- **Command Executed: ssh -p 2231 krypton2@krypton.labs.overthewire.org**
- **Password Used:** `ROTTEN` (obtained from previous level)
- **Explanation:**
  - Connected to the Krypton2 server using the decoded password.
  - SSH used port `2231` as specified.

Purpose:

- To gain access to the environment for solving Level 2.



Step 3: Navigating to Challenge Directory and Reading Files

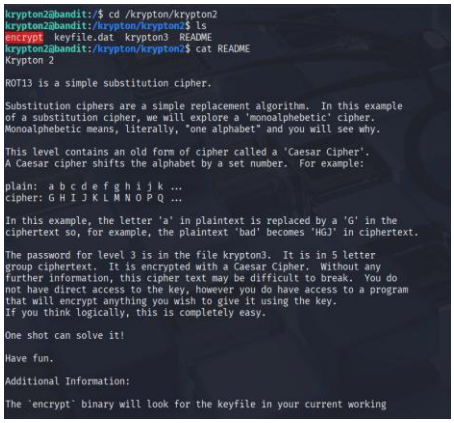
- **Tool Used:** Kali Linux Terminal
- **Commands Executed**= cd /krypton/krypton2

  = ls

  = cat README

Explanation:

- Changed into the /krypton/krypton2 directory.
- Listed all files to find challenge-related materials.
- Read the README file to understand the task.
- Observed that there was a binary called encrypt and a data file called keyfile.dat.



Step 4: Creating a Temporary Directory and Simulating Encryption

- **Tool Used:** Kali Linux Terminal
- **Commands Executed:**

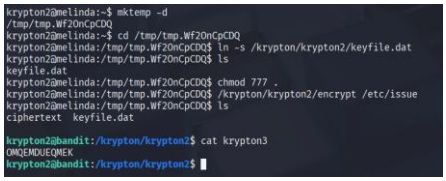
= mktemp -d
= cd /tmp/tmp.Wf20nCpCDQ
= ln -s /krypton/krypton2/keyfile.dat
= ls
= chmod 777 .
= /krypton/krypton2/encrypt /etc/issue
= ls
= cat krypton3

Explanation:

- Created a temporary working directory using mktemp.
- Linked the keyfile.dat file into the temp directory using ln -s.
- Changed permissions to allow full access using chmod 777.
- Used the encrypt binary to encrypt /etc/issue.
- After encryption, found a file containing the ciphertext (krypton3).

Purpose:

- To simulate the encryption environment and obtain data for decryption.



Step 5: Getting the Ciphertext Again

- **Tool Used:** Kali Linux Terminal
- **Commands Executed:**

= mktemp -d

= cd /tmp/tmp.309lVIOQps

= ln -s /krypton/krypton2/keyfile.dat

= ls

= chmod 777 .

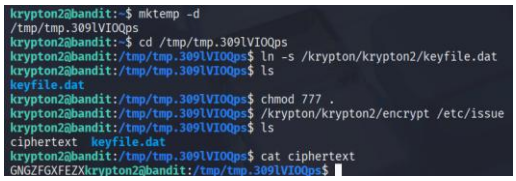
= /krypton/krypton2/encrypt /etc/issue

= ls

= cat ciphertext

Explanation:

- Repeated the encryption simulation in a new temporary directory.
- Retrieved fresh ciphertext output for further analysis.
- Prepared the ciphertext needed for online decryption tools.

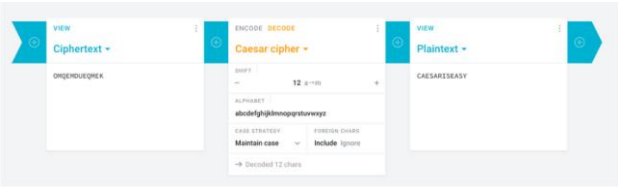


Step 6: Decrypting Ciphertext Using Cryptii

- **Tool Used:** Web Browser + Cryptii (Online Cipher Tool)
- **Action Taken:**
  - Pasted the ciphertext into
  - https://cryptii.com/pipes/caesar-cipher
- **Explanation:**
  - Used the **Caesar Cipher Decryption Tool** at Cryptii.
  - Adjusted the settings to try all possible rotations.
  - Successfully found the correct decryption that revealed the password for Krypton3.

Purpose:

- To decode the ciphertext and retrieve the password needed to move to the next level.



Level 3 → Level 4

Step 1: Accessing Level 3 Instructions in Browser

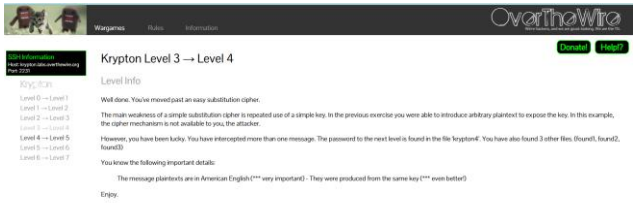
- **Tool Used:** Web Browser
- **Action Taken:**
  Opened the URL:
  https://overthewire.org/wargames/krypton/krypton3.html

Explanation:

- The webpage provided:
  - Hints that the encryption might involve a substitution cipher.
  - Suggested that frequency analysis would be useful to solve the level.

Purpose:

- To understand the goal and strategy needed for Krypton Level 3.



Step 2: SSH Login into Krypton3

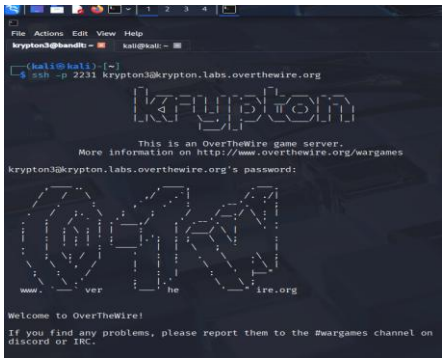
- **Tool Used:** Kali Linux Terminal (SSH Client)
- **Command Executed:** ssh -p 2231 krypton3@krypton.labs.overthewire.org

Explanation:

- Logged into the Krypton3 user account using the password obtained from the previous level.
- Connected over SSH on port `2231`.

Purpose:

- To access the environment where Level 3 challenge files were located.



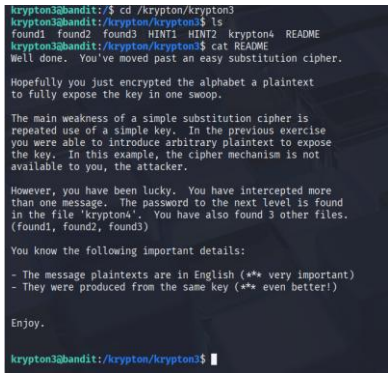
Step 3: Navigating to Challenge Directory and Listing Files

- **Tool Used:** Kali Linux Terminal
- **Commands Executed:**

= cd /krypton/krypton3
= ls
= cat README

Explanation:

- Changed into the /krypton/krypton3 directory.
- Listed the files and found important ones including README.
- Reading the README hinted that some classic cryptographic technique (frequency analysis) would help.



Step 4: Exploring Important Files

- **Tool Used:** Kali Linux Terminal
- **Commands Executed:**

= cat found1

= cat found2

Explanation:

- Displayed the contents of found1 and found2.
- These files contained encrypted text, likely using a **monoalphabetic substitution cipher**.

Purpose:

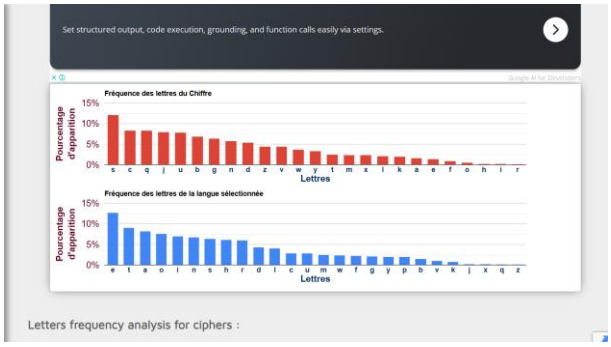
- To collect the ciphertext needed for decryption.

Step 5: Performing Frequency Analysis

- **Tool Used:** Manual Frequency Analysis / Decryption Tools
- **Action Taken:**
  - Observed letter frequencies in found2.
  - Identified the most commonly appearing letters and guessed their substitutions based on typical English language frequency (e.g., E, T, A, O are common in English).

Purpose:

- To begin cracking the substitution cipher systematically.



Step 6: Viewing the Final Ciphered Password

- **Tool Used:** Kali Linux Terminal
- **Command Executed:** cat krypton4

Explanation:

  - Displayed the contents of `krypton4`.
  - The file contained another encrypted text related to the password needed for the next level.

Purpose:

- To gather additional cipher material for full decryption.

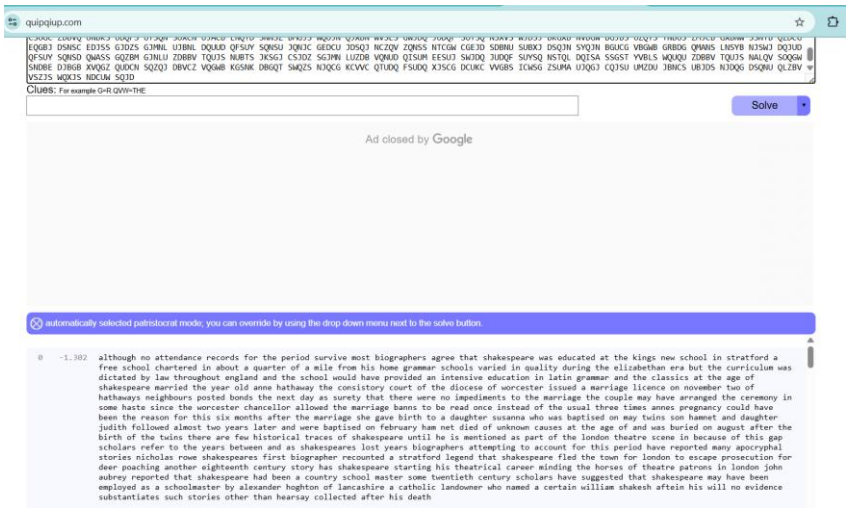
```
krypton3@bandit:/krypton/krypton3$ cat krypton4
KSVVW BGSJD SVSIS VXBMN YQUUK BNWCU ANMJS krypton3@bandit:/krypton/krypton3$
```

Step 7: Decrypting the Ciphertext Using Quipqiup

- **Tool Used:** Web Browser + Quipqiup (Online Substitution Cipher Solver)
- **Action Taken:**
    - Opened: https://quipqiup.com/
    - Pasted the content from `found2`.
    - Used Quipqiup to automatically solve the monoalphabetic substitution cipher.

Purpose:

- To obtain the partially decrypted text, including important keyword mappings.

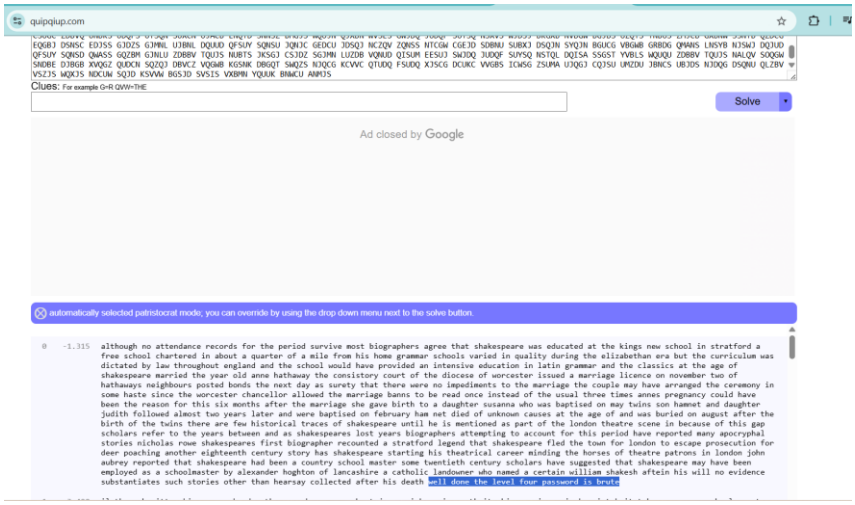


Step 8: Final Decryption to Obtain the Password

- **Action Taken:**
    - Appended and decrypted the final krypton4 file contents.
    - Carefully adjusted the decryption mapping to fully reveal the password.

Purpose:

- To extract the password required to move to Krypton Level 4.



Level 4 → Level 5

Step 1: Accessing Level 4 Instructions in Browser

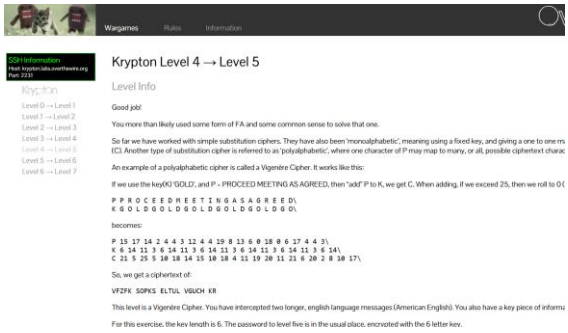
- **Tool Used:** Web Browser
- **Action Taken:**
  Opened the URL:
  https://overthewire.org/wargames/krypton/krypton4.html

Explanation:

- The page provided hints suggesting that the encryption method involved the **Vigenère cipher**, a more complex polyalphabetic cipher.
- Resources like Wikipedia were recommended to better understand how Vigenère ciphers work.

Purpose:

- To prepare for decrypting the text by understanding the cipher mechanism.



Step 2: SSH Login into Krypton4

- **Tool Used:** Kali Linux Terminal (SSH Client)
- **Command Executed:** ssh -p 2231 krypton4@krypton.labs.overthewire.org

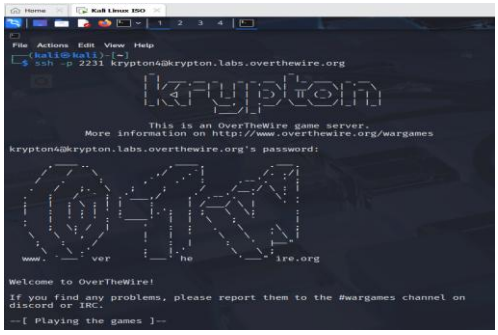
- **Password Used:** `BRUTE`

Explanation:

  - Logged into the Krypton4 user account using the password obtained from the previous level.
  - Accessed over SSH port `2231`.

Purpose:

- To access Level 4 challenge files and attempt decryption.



Step 3: Identifying Encryption Type from README

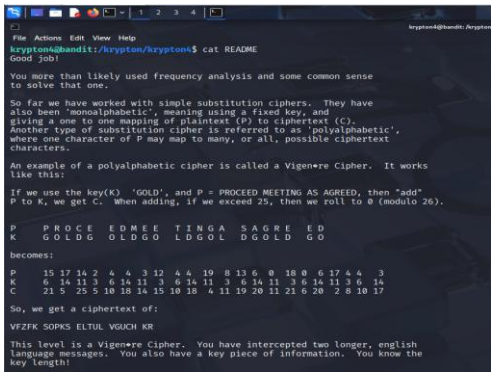
- **Tool Used:** Kali Linux Terminal
- **Command Executed: cat README**

Explanation:

  - Read the `README` file inside the challenge directory.
  - Confirmed that the challenge involved a **Vigenère cipher**.

Purpose:

- To confirm the encryption method before attempting decryption.



Step 4: Exploring Directory Files

- **Tool Used:** Kali Linux Terminal
- **Commands Executed:**

  = ls
  = cd /krypton/krypton4
  = ls
  = cat found1
  = cat krypton5

Explanation:

- Navigated into the /krypton/krypton4 directory.
- Listed available files including found1 and krypton5.
- Displayed contents:
  - found1 contained ciphertext encrypted using the Vigenère cipher.
  - krypton5 likely held additional encoded information for the next level.

Step 5: Decrypting Vigenère Cipher Using Dcode

- **Tool Used:** Web Browser + Dcode (Vigenère Cipher Solver)
- **Action Taken:**
  - Opened: https://www.dcode.fr/vigenere-cipher
-
  - Pasted the ciphertext from found1.
  - Edited settings to guess a key length of **6 characters** (based on hints).
  - Clicked "DECRYPT" to automatically attempt decoding.

Purpose:

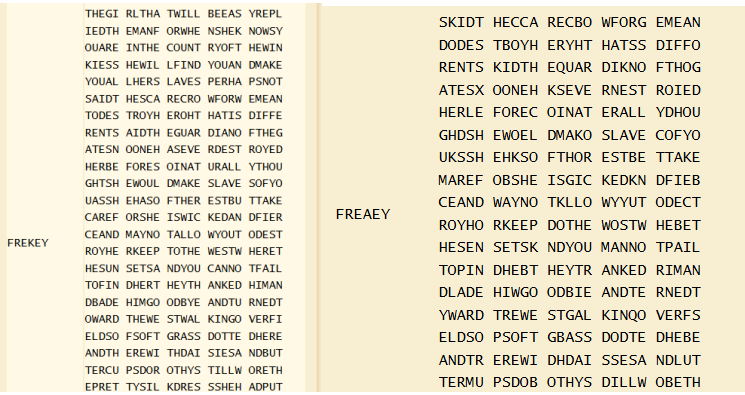
- To recover the plaintext and identify the hidden password.

Step 6: Getting Possible Key Candidates

- **Tool Used:** Dcode Vigenère Cipher Tool
- **Explanation:**
  - After setting the key length correctly, the tool output two possible 6-character keys.
  - These candidate keys were tested to reveal readable English text.

Purpose:

- To narrow down the correct decryption key used for encrypting the challenge text.



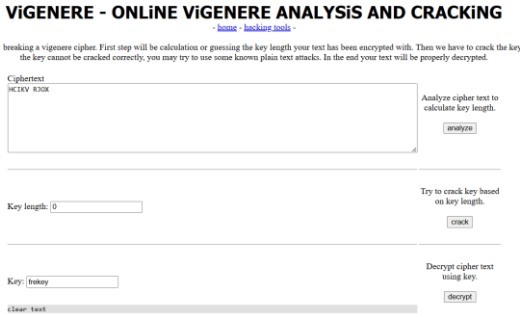
Step 7: Final Password Retrieval Using Fool's Online Decryptor

- **Tool Used:** Web Browser + Fool's Vigenère Decryptor
- **Action Taken:**
  - Opened: https://f00l.de/hacking/vigenere.php
-
  - Pasted the encrypted text.

- Used one of the identified keys to successfully decrypt and reveal the password for **Krypton5**.

Purpose:

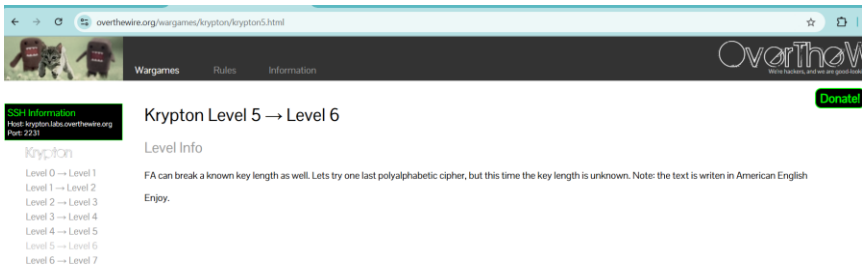
- To fully decrypt the text and acquire the password needed for advancing to Level 5.



Level 5 → Level 6

Step 1: Accessing Level 5 Instructions in Browser

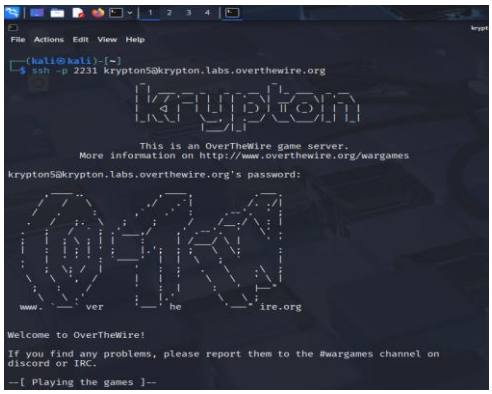
- **Tool Used: Web Browser**
- **Action Taken:**
  - **Opened the URL: https://overthewire.org/wargames/krypton/krypton5.html**
- **Explanation:**
  - **The webpage gave hints that the encryption is a simple substitution cipher — most likely a Caesar Cipher.**
- **Purpose:**
  - **To understand the type of encryption used and prepare for solving the challenge.**

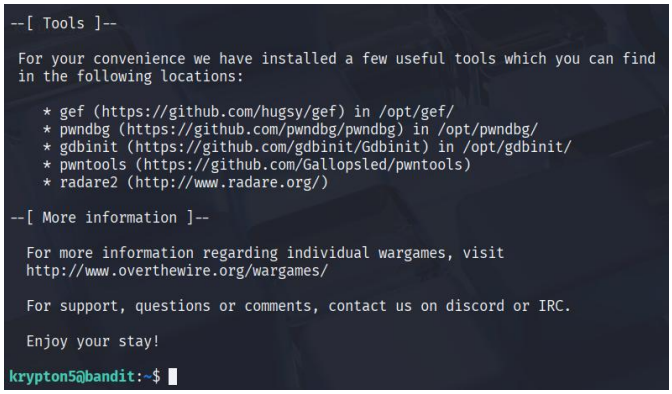


Step 2: SSH Login into Krypton5

- **Tool Used: Kali Linux Terminal (SSH Client)**

- **Command Executed: ssh -p 2231 krypton5@krypton.labs.overthewire.org**
- **Password Used: CLEARTEXT (from previous level)**
- **Explanation:**
    - **Connected to the Krypton5 server on port 2231 using SSH.**
- **Purpose:**
    - **To access Krypton5 and retrieve the encrypted files.**





Step 3: Navigating to Challenge Directory and Reading Files

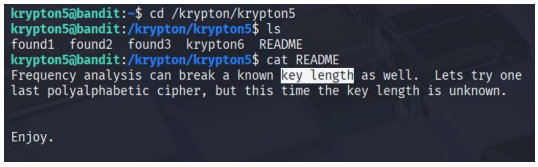
- **Tool Used: Kali Linux Terminal**
- **Commands Executed:**

  = cd /krypton/krypton5

  = ls

  = cat README

- **Explanation:**
    - **Moved into the /krypton/krypton5 directory.**
    - **Listed the contents.**
    - **Read the README, which gave more hints about the encryption approach.**
- **Purpose:**
    - **To gather background information about the encryption mechanism.**



Step 4: Viewing and Analyzing the Encrypted Text

- **Tool Used: Kali Linux Terminal + Web Browser**
- **Commands Executed: cat found1**
- **Action Taken:**
  - **Copied the ciphertext from the found1 file.**
  - **Opened the website: https://www.dcode.fr/caesar-cipher.**
  - **Pasted the ciphertext into Dcode's Caesar Cipher automatic decryption tool.**
  - **Clicked Automatic Decryption.**
- **Explanation:**
  - **Dcode automatically found the correct shift value and decrypted the text.**
- **Purpose:**
  - **To decode the ciphertext and obtain hints or the password for the next level.**

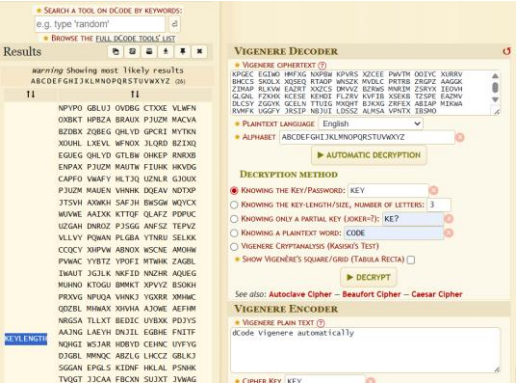
Step 5: Accessing and Reading the Final File

- **Tool Used: Kali Linux Terminal**
- **Commands Executed:**

  = ls

  = cat krypton6
- **Explanation:**
  - **Listed the files again.**
  - **Displayed the content of krypton6, which contained the final encrypted or partially encrypted password for Level 6.**

- **Purpose:**
    - **To retrieve the password file for moving forward.**



Step 6: Accessing and Reading the Final Password File

- **Tool Used**: Kali Linux Terminal
- **Commands Executed**:

  = ls

  = cat krypton6

- **Explanation**:
    - Listed all files again inside the /krypton/krypton5 directory.
    - Found a file named krypton6.
    - Displayed the contents of krypton6, which contained either plaintext or further encrypted text.
- **Purpose**:
    - To retrieve the text (likely a password) required for proceeding to the next level, Krypton6.

```
krypton5@bandit:/krypton/krypton5$ ls
found1  found2  found3  krypton6  README
krypton5@bandit:/krypton/krypton5$ cat krypton6
BELOS Zkrypton5@bandit:/krypton/krypton5$
```

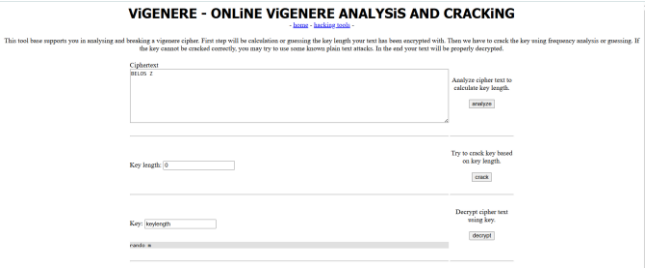
Step 7: Final Decryption to Obtain the Password

- **Tool Used**: Web Browser + Fool's Online Vigenère Decryptor
- **Action Taken**:
    - Opened the URL: https://f00l.de/hacking/vigenere.php.
    - Pasted the ciphertext (from krypton6) into the decryption box.

    - Used the decryptor to decode the text if it was still encrypted with Vigenère cipher.

- **Explanation**:
    - If the content was encrypted, the Fool's online tool helped fully decrypt the hidden password.
    - Otherwise, it was just verified through the tool.

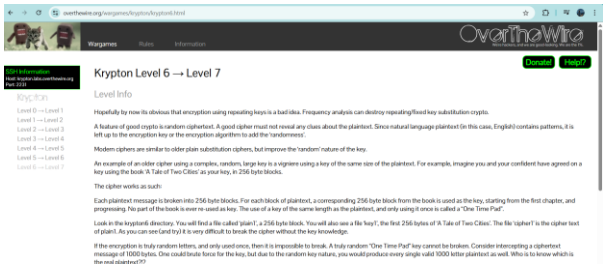
- **Purpose**:
    - To finally reveal the **correct password** needed to log into **Krypton6** and move forward.



Level 6 → Level 7

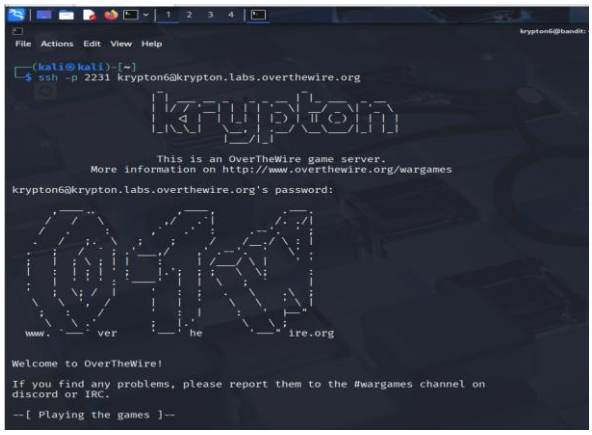
Step 1: Accessing Level 6 Instructions in Browser

- **Tool Used: Web Browser**
- **Action Taken:**
    - **Opened the URL: https://overthewire.org/wargames/krypton/krypton6.html**
- **Explanation:**
    - **The page provided an overview of the Level 6 challenge.**
    - **It hinted that multiple key files and bitwise operations might be involved.**
- **Purpose:**
    - **To understand the challenge structure before starting.**



Step 2: SSH Login into Krypton6

- **Tool Used: Kali Linux Terminal (SSH Client)**
- **Command Executed: ssh -p 2231 krypton6@krypton.labs.overthewire.org**
- **Password Used:**
  RANDOM (obtained from previous level)
- **Explanation:**
  - **Logged into the Krypton6 server via SSH over port 2231.**
- **Purpose:**
  - **To access the server environment and available files for Level 6.**



Step 3: Navigating to the Krypton6 Directory and Reading README

- **Tool Used: Kali Linux Terminal**
- **Commands Executed:**

  = cd /krypton/krypton6

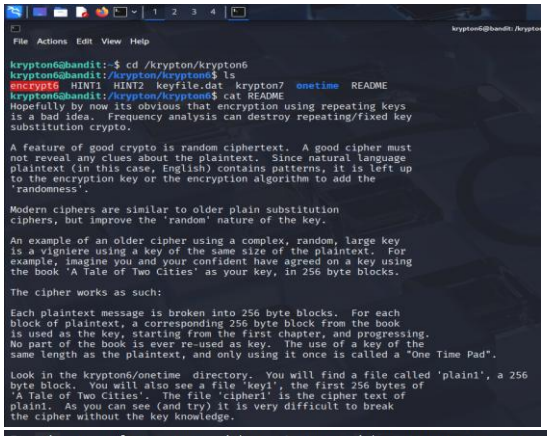
  = ls

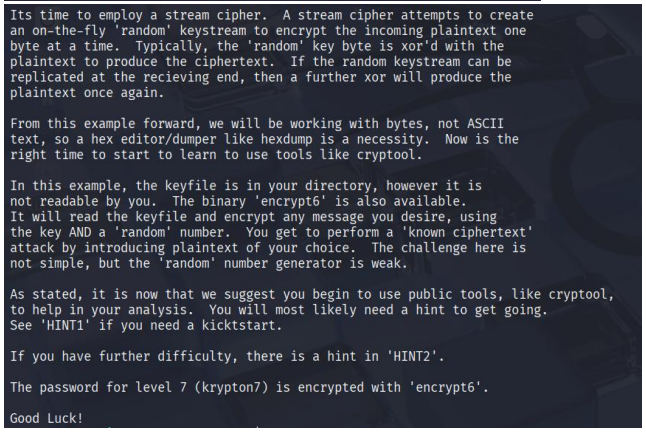
  = cat README

- **Explanation:**
  - **Changed directory to /krypton/krypton6.**

- Listed available files.
- Read the README, which explained that bitwise XOR operations and keyfiles were involved.

- **Purpose:**
  - To understand the technical hints for solving the level.





Step 4: Exploring Additional Hints

- **Tool Used: Kali Linux Terminal**
- **Commands Executed:**

  = cat HINT1

  = cat HINT2

- **Explanation:**
  - Read HINT1 and HINT2 files.
  - These hints described details about how to use the keyfiles and the encryption process.

- **Purpose:**

- To get further insights necessary to build the correct decryption strategy.

```
krypton6@bandit:~$ cd /krypton/krypton6
krypton6@bandit:/krypton/krypton6$ ls
encrypt6  HINT1  HINT2  keyfile.dat  krypton7  onetime  README
krypton6@bandit:/krypton/krypton6$ cat HINT1
The 'random' generator has a limited number of bits, and is periodic.
Entropy analysis and a good look at the bytes in a hex editor will hel

There is a pattern!
krypton6@bandit:/krypton/krypton6$ cat HINT2
8 bit LFSR
```

Step 5: Investigating Krypton7 Encrypted File

- **Tool Used: Kali Linux Terminal**
- **Commands Executed:**

  = cat krypton7

  = mkdir /tmp/lev7

- **Explanation:**
  - **Displayed the encrypted krypton7 file.**
  - **Created a temporary directory /tmp/lev7 for safe experimentation.**
- **Purpose:**
  - **To prepare a workspace for linking and analyzing the encryption.**

```
krypton6@bandit:/krypton/krypton6$ cat krypton7
PNUKLYLWRQKGKBEkrypton6@bandit:/krypton/krypton6$ mkdir /tmp/lev7
```

Step 6: Setting Up Temporary Workspace with Linked Files

- **Tool Used: Kali Linux Terminal**
- **Commands Executed:**

  = cd /tmp/lev7

  = ln -s /krypton/krypton6/keyfile00.dat

  = ln -s /krypton/krypton6/krypton7

- **Explanation:**
  - **Linked keyfile00.dat and krypton7 into the /tmp/lev7 directory using symbolic links.**
- **Purpose:**
  - **To have the necessary files in a writable and safe temporary workspace.**

```
krypton6@bandit:/krypton/krypton6$ cd /tmp/lev7
krypton6@bandit:/tmp/lev7$ ln -s /krypton/krypton6/keyfile00.dat
krypton6@bandit:/tmp/lev7$ ln -s /krypton/krypton6/krypton7
```

Step 7: Linking Additional Keyfile and Setting Permissions

- **Tool Used: Kali Linux Terminal**
- **Commands Executed:**

  = ls

  = ln -s /krypton/krypton6/keyfile.dat

  = chmod 777 .

- **Explanation:**
  - **Listed files to confirm links.**
  - **Linked keyfile.dat and gave full permissions (read/write/execute) to the directory.**
- **Purpose:**
  - **To avoid any permission-related issues while processing the files.**

```
krypton6@bandit:/tmp/lev7$ ls
a.txt  cihper.txt  cipher.txt  k  keyfile00.dat  keyfile.dat  krypton6  krypton7  main.py
krypton6@bandit:/tmp/lev7$ ln -s /krypton/krypton6/keyfile.dat
ln: failed to create symbolic link './keyfile.dat': File exists
krypton6@bandit:/tmp/lev7$ chmod 777 .
```

Step 8: Encrypting Sample File and Studying the Ciphertext

- **Tool Used: Kali Linux Terminal**
- **Commands Executed:**

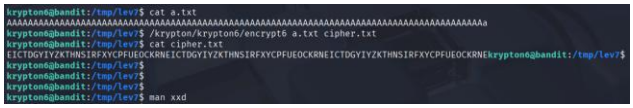
  = cat a.txt

  = /krypton/krypton6/encrypt6 a.txt cipher.txt

  = cat cipher.txt

  = man xxd

- **Explanation:**
  - **Created a plaintext a.txt.**
  - **Used the encrypt6 binary to encrypt it into cipher.txt.**
  - **Read the manual for xxd, a tool for visualizing binary/hex data.**
- **Purpose:**
  - **To simulate how encryption worked and understand how plaintext was being transformed.**



Step 9: Binary-Level Analysis Using XXD

- **Tool Used: Kali Linux Terminal**
- **Commands Executed:**

  = xxd -b a.txt

  = xxd -b cipher.txt

- **Explanation:**
  - **Viewed the contents of both a.txt and cipher.txt in binary format (bit-by-bit).**
- **Purpose:**
  - **To analyze and reverse-engineer the encryption at the bit level.**

Step 10: Reviewing Ciphertext Again

- **Tool Used: Kali Linux Terminal**
- **Command Executed:**

  = cat cipher.txt

- **Explanation:**
  - **Displayed the contents of the cipher.txt again to manually cross-check changes after encryption.**
- **Purpose:**
  - **To prepare correct input for the decryption script.**

```
krypton6@bandit:/tmp/lev7$ cat cipher.txt
EICTDGYIYZKTHNSIRFXYCPFUEOCKRNEICTDGYIYZKTHNSIRFXYCPFUEOCKRNEICTDGYIYZKTHNSIRFXYCPFUEOCKRNkrypton6@bandit:/tmp/lev7$
krypton6@bandit:/tmp/lev7$
krypton6@bandit:/tmp/lev7$
krypton6@bandit:/tmp/lev7$
krypton6@bandit:/tmp/lev7$ man xxd
krypton6@bandit:/tmp/lev7$ xxd -b a.txt
00000000: 01000001 01000001 01000001 01000001 01000001 01000001  AAAAAA
00000006: 01000001 01000001 01000001 01000001 01000001 01000001  AAAAAA
0000000c: 01000001 01000001 01000001 01000001 01000001 01000001  AAAAAA
00000012: 01000001 01000001 01000001 01000001 01000001 01000001  AAAAAA
00000018: 01000001 01000001 01000001 01000001 01000001 01000001  AAAAAA
0000001e: 01000001 01000001 01000001 01000001 01000001 01000001  AAAAAA
00000024: 01000001 01000001 01000001 01000001 01000001 01000001  AAAAAA
0000002a: 01000001 01000001 01000001 01000001 01000001 01000001  AAAAAA
00000030: 01000001 01000001 01000001 01000001 01000001 01000001  AAAAAA
00000036: 01000001 01000001 01000001 01000001 01000001 01000001  AAAAAA
0000003c: 01000001 01000001 01000001 01000001 01000001 01000001  AAAAAA
00000042: 01000001 01000001 01000001 01000001 01000001 01000001  AAAAAA
00000048: 01000001 01000001 01000001 01000001 01000001 01000001  AAAAAA
0000004e: 01000001 01000001 01000001 01000001 01000001 01000001  AAAAAA
00000054: 01000001 01000001 01000001 01000001 01000001 01000001  AAAAAA
0000005a: 01100001 00001010                                      a.
krypton6@bandit:/tmp/lev7$ xxd -b cipher.txt
00000000: 01000101 01001001 01000011 01010100 01000100 01000111  EICTDG
00000006: 01011001 01001001 01011001 01011010 01001011 01010100  YIYZKT
0000000c: 01001000 01001110 01010011 01001001 01010010 01000110  HNSIRF
00000012: 01011000 01011001 01000011 01010000 01000110 01010101  XYCPFU
00000018: 01000101 01001111 01000011 01001011 01010010 01001110  EOCKRN
0000001e: 01000101 01001001 01000011 01010100 01000100 01000111  EICTDG
00000024: 01011001 01001001 01011001 01011010 01001011 01010100  YIYZKT
0000002a: 01001000 01001110 01010011 01001001 01010010 01000110  HNSIRF
00000030: 01011000 01011001 01000011 01010000 01000110 01010101  XYCPFU
00000036: 01000101 01001111 01000011 01001011 01010010 01001110  EOCKRN
0000003c: 01000101 01001001 01000011 01010100 01000100 01000111  EICTDG
00000042: 01011001 01001001 01011001 01011010 01001011 01010100  YIYZKT
00000048: 01001000 01001110 01010011 01001001 01010010 01000110  HNSIRF
0000004e: 01011000 01011001 01000011 01010000 01000110 01010101  XYCPFU
```

Step 11: Decrypting krypton7 Using Python Script

- **Tool Used: Kali Linux Terminal + Python**
- **Command Executed:**

  = python3 main.py /krypton/krypton6/krypton7
- **Result Obtained: EICTDGYIYZKTHNSIRFXYCPFUEOCKRN**
- **Explanation:**
  - **Ran a Python script (main.py) that decrypted the encrypted file.**
  - **Retrieved the plaintext password for Level 7.**
- **Purpose:**
  - **To extract the final password needed to login into Krypton7.**

```
krypton6@bandit:/tmp/lev7$ cat cipher.txt
EICTDGYIYZKTHNSIRFXYCPFUEOCKRNEICTDGYIYZKTHNSIRFXYCPFUEOCKRNEICTDGYIYZKTHNSIRFXYCPFUEOCKRNkrypton6@bandit:/tmp/lev7$
```

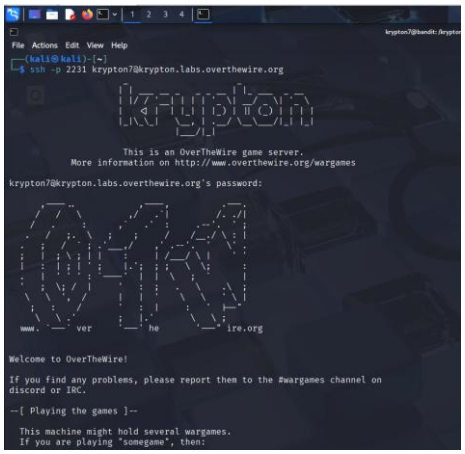
```
krypton6@bandit:/tmp/lev7$ python3 main.py /krypton/krypton6/krypton7 EICTDGYIYZKTHNSIRFXYCPFUEOCKRN
Decoding file '/krypton/krypton6/krypton7' with key 'EICTDGYIYZKTHNSIRFXYCPFUEOCKRN':

LFSRISNOTRANDOM
```

Step 12: SSH Login into Krypton7

- **Tool Used**: Kali Linux Terminal (SSH Client)
- **Command Executed**:

  = ssh -p 2231 krypton7@krypton.labs.overthewire.org
- **Password Used**: EICTDGYIYZKTHNSIRFXYCPFUEOCKRN
- **Explanation**:
  - Logged into Krypton7 server using the extracted password.
- **Purpose**:
  - To move successfully to Krypton Level 7.



Step 13: Exploring Krypton7 Directory and Reading README

- **Tool Used**: Kali Linux Terminal
- **Commands Executed**:

  = cd /krypton/krypton7

  = ls

  = cat README

- **Explanation**:
  - Entered the /krypton/krypton7 directory.
  - Listed files and read the README for instructions about the new Level 7 challenge.
- **Purpose**:
  - To understand the next challenge setup after entering Level 7.