

REPORT – KRYPTON

Basic Commands

- ssh – Connect to the OverTheWire server.
- cd, ls, cat – Navigate directories and read files.
- echo – Print text (used for passing inputs).
- nano / vim – Edit files (for custom plaintext attacks).
- mktemp -d – Create temporary directories.
- ln -s – Create symbolic links (for accessing restricted files).
- chmod – Modify file permissions.

Cryptography Tools

- base64 – Decode Base64-encoded strings.
- tr – Translate characters (used for Caesar cipher decryption).

Level 0 → Level 1

Objective: Decode a Base64-encoded password.

Steps to execute:

1. Decode the password:

```
echo "S1JZUFRPTkITR1JFQVQ=" | base64 -d
```

- base64 -d decodes the given string.
- Output: KRYPTONISGREAT (password for Level 1).

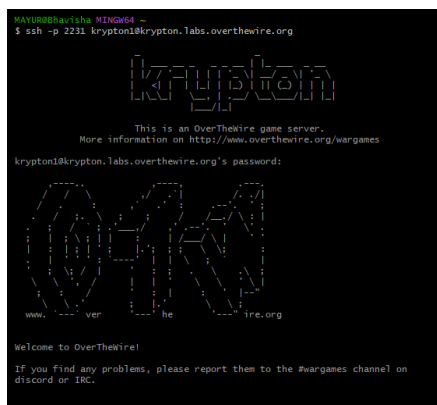
2. SSH into Level 1:

```
ssh -p 2231 krypton1@krypton.labs.overthewire.org
```

- Password: KRYPTONISGREAT.

Logic:

- Base64 is not encryption but encoding—easily reversible.



Level 1 → Level 2

Objective: Decrypt a ROT13 (Caesar shift) cipher.

Steps to execute:

1. Navigate to the level directory:

```
cd /krypton/krypton1
```

2. List files (README and krypton2).
3. Read the README file for hints.
4. View the encrypted password:

```
cat krypton2
```

- Output: YRIRY GJB CNFFJBEQ EBGGRA

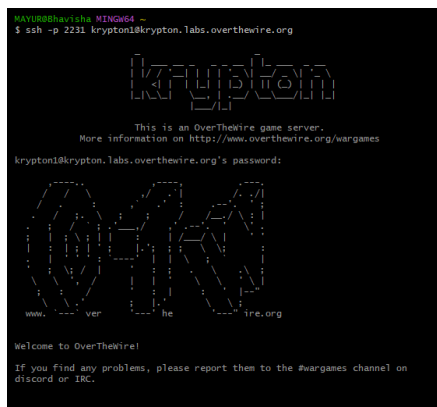
5. Decrypt using tr (ROT13):

```
cat krypton2 | tr "[A-Z]" "[N-ZA-M]"
```

- Output: LEVEL TWO PASSWORD ROTTEN

Logic:

- ROT13 shifts each letter by 13 positions.
- tr maps [A-Z] to [N-ZA-M] (N-Z covers A-M shifted, and A-M covers N-Z shifted).



Level 2 → Level 3

Objective: Break a fixed-key substitution cipher using a known-plaintext attack.

Steps to execute:

1. Navigate to the level directory:

```
cd /krypton/krypton2
```

2. Read README – It explains that an encryption program (encrypt) uses a fixed key.
3. Create a temporary directory to work in:

```
mktemp -d
```

```
cd /tmp/tmp.randomstring
```

4. Link the keyfile (required for encryption):

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

5. Allow write permissions:

```
chmod 777 .
```

6. Test encryption:

```
/krypton/krypton2/encrypt /etc/issue
```

- Creates ciphertext.

7. Create a custom plaintext file (ptext) with known content (e.g., AAAAA):

```
echo "AAAAA" > ptext
```

```
/krypton/krypton2/encrypt ptext
```

8. Compare ciphertext with ptext to deduce the shift.

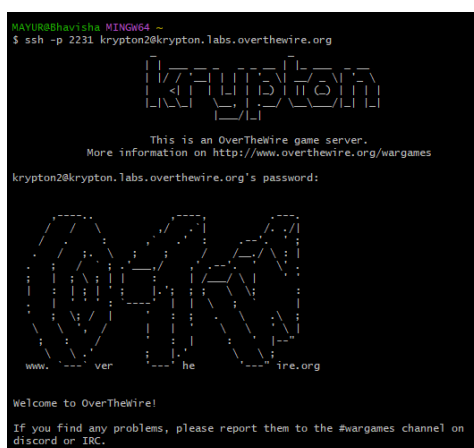
9. Decrypt the password file:

```
cat /krypton/krypton2/krypton3 | tr "[M-ZA-L]" "[A-Z]"
```

- Output: CAESARISEASY

Logic:

- The encrypt program uses a fixed Caesar shift.
- By encrypting known plaintext (AAAAA), we can determine the shift amount.
- tr reverses the shift (here, it was a shift of 12).



Level 3 → Level 4

Objective: Decrypt another ROT13 cipher.

Steps to execute :

1. SSH into Level 3:

```
ssh -p 2231 krypton3@krypton.labs.overthewire.org
```

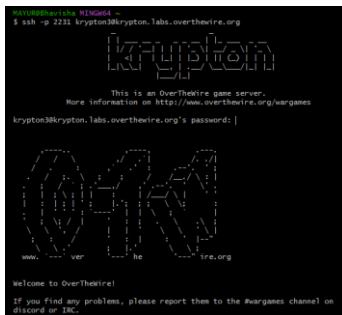
2. Navigate to /krypton/krypton3.
3. Read krypton4 (encrypted password).
4. Decrypt using ROT13:

```
cat krypton4 | tr 'A-Z' 'N-ZA-M'
```

- Output: BRUTE

Logic:

- Same as Level 1, but with a different password.



Level 4 → Level 5

Objective: Break a substitution cipher using frequency analysis.

Steps to execute:

1. SSH into Level 4.
2. Navigate to /krypton/krypton4.
3. Copy the encrypted password to a file:

```
cat krypton5 > cipher.txt
```

4. Analyze letter frequencies manually (compare to English: E, T, A, O, etc.).
5. Substitute letters based on frequency patterns.

Logic:

- Unlike Caesar cipher, this is a **general substitution cipher**.
- Requires manual frequency analysis (e.g., most common letter → "E").

```
RAY000@hawaii:~$ ssh -p 2231 krypton4@krypton.labs.overthewire.org
krypton
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames
krypton4@krypton.labs.overthewire.org's password:
www. ver he ire.org
Welcome to OverTheWire!
If you find any problems, please report them to the #wargames channel on
discord or IRC.
```

Level 5 → Level 6

Objective: Break a more complex cipher (likely Vigenère).

Steps:

1. SSH into Level 5.
2. Navigate to /krypton/krypton5.
3. Analyze krypton6 ciphertext.
4. Use **Kasiski examination** to find key length.
5. Perform frequency analysis on each key segment.

Logic:

- Vigenère uses a keyword; finding repeating sequences helps determine key length.
- Once key length is known, each segment can be treated as a Caesar cipher.

```
RAY000@hawaii:~$ ssh -p 2231 krypton5@krypton.labs.overthewire.org
krypton
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames
krypton5@krypton.labs.overthewire.org's password:
www. ver he ire.org
Welcome to OverTheWire!
If you find any problems, please report them to the #wargames channel on
discord or IRC.
```

Level 6 → Level 7:

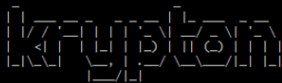
Objective: Decrypt a ciphertext (similar to Level 4).

Tools: Frequency analysis or scripting

Steps:


- Logic:** Longer ciphertexts allow for more sophisticated attacks like Kasiski examination to determine the key length and decrypt the password.

```
MAYUR@Bhavisha MINGw64 ~  
$ ssh -p 2231 krypton6@krypton.labs.overthiwire.org
```



This is an OverTheWire game server.
More information on <http://www.overthiwire.org/wargames>

krypton6@krypton.labs.overthiwire.org's password:



www. ver he ire.org

Welcome to OverTheWire!

If you find any problems, please report them to the #wargames channel on discord or IRC.