

Operation Foresty

Player: constantine

Kategori: Cryptography

Challenge

13 Solves



Operation FORESTY - Macam-Macam Tipe Enkripsi Klasik

320

Medium-Hard

FORESTY - Forensic and Security Laboratory - sedang melakukan simulasi CTF untuk calon anggota Study Group 2025. Dalam salah satu chall, sebuah pesan penting telah dikunci menggunakan enkripsi berlapis enam yang seluruhnya menggunakan teknik kriptografi klasik.

Diketahui pesan terenkripsi sebagai berikut:

GAHQCMCVFWJUAIDEISRZWTMUCUJUSFDMYIGP

Flag format: *FORESTY{x_x_x_x}*

author: Tyzals

View Hint

View Hint

View Hint

Flag

Submit

Phase 1: Recon

Challenge ini menggunakan **multi-layer classical cryptography**. Tahapan penting sebelum memulai adalah **menganalisis urutan cipher yang digunakan**, sebab proses dekripsi harus dilakukan **dengan urutan terbalik (reverse pipeline)**.

Dari soal, urutan enkripsi adalah:

1. **Columnar Transposition** - **key: TRAFFIC**
2. **Hill Cipher 2x2** - **matrix: $\begin{bmatrix} 11 & 11 \end{bmatrix}$**
3. **Affine Cipher** - **$a = 3, b = 5$**
4. **Vigenère Cipher** - **key: HASH**
5. **Custom Substitution** - alfabet dibangun dari FORESTY + sisa alfabet
6. **ROT13** - lapisan terakhir

Maka urutan dekripsi menjadi:

- ROT13
- Custom Substitution
- Vigenère (decrypt)
- Affine (decrypt)
- Hill Cipher (matrix inverse)
- Columnar Transposition (decrypt)

Phase 2: Layer-by-Layer Execution

ROT13

Di CyberChef cukup tambahkan operation ROT13, udah default aja.

Masih unreadable: TNUDPZPISJWHNVQRVFEMJGZHPHWHFSQZLVTC

Custom Substitution

Dari clue kedua, alfabet kustom dibentuk dari kata "FORESTY" + sisa huruf alfabet.

Alphabet hasil: FORESTYABCDGHIJKLMNOPQUVWXZ

Di CyberChef:

```
Substitute → From: FORESTYABCDGHIJKLMNOPQUVWXZ → To:  
ABCDEFGHIJKLMNQRSTUUVWXYZ
```

Masih unreadable: FSVKTZTNEOXMSWUCWADROLZMTMXMAEUZQWFJ

Vigenère Decode

Set mode decrypt, bagian key masukan HASH.

Masih unreadable: YSDDMZBGXOFFLWCVPALKHLHFMMFFTECSJWNC

Affine Decode

Affine di CyberChef langsung set:

```
a = 3  
b = 5  
mode = Decrypt
```

Masih unreadable: PNILYQJGDAAACXZOMHCTSCSALLAAWRZNXUZ

Hill Cipher Decrypt

Matrix dari clue:

```
7 8  
11 11
```

CyberChef gapunya di bagian ini, jadi aku pindah ke dcode.fr.

Masukkan ciphertext hasil layer affine → pilih decrypt → isi matrix. Masih kebentuk transposed.

Search for a tool

★ SEARCH A TOOL ON dCode

e.g. type 'sudoku'

★ BROWSE THE FULL dCODE TOOLS' LIST

Results

PNIIYQJGDAACXZOMHCTSCSALLAAWRZNXUZ

7 8
11 11

=ABCDEFGHIJKLMNOPQRSTUVWXYZ

LCMKXRAPIXAAKLXJMRAXAMISXEAAXBMCTKX

Hill Cipher - dCode

Tag(s) : Poly-Alphabetic Cipher

Share

dCode and more

HILL DECODER

★ HILL CIPHERTEXT

PNIIYQJGDAACXZOMHCTSCSALLAAWRZNXUZ

☐ TRY/BRUTEFORCE ALL 2x2 MATRIX (VALUES < 10 + LATIN ALPHABET)

☒ I KNOW THE NxN MATRIX NUMBERS/VALUES

7 8 2 x 2 RESIZE
11 11 CLEAR
FILL WITH 0
FILL WITH 1

☒ ALPHABET (26 LET. A=0) ABCDEFGHIJKLMNOPQRSTUVWXYZ

☐ ALPHABET (26 LET. A=1) ZABCDEFGHIJKLMNOPQRSTUVWXYZ

☐ ALPHABET (27 CHAR. A=0) ABCDEFGHIJKLMNOPQRSTUVWXYZ_

☐ ALPHABET (27 CHAR. A=1) _ABCDEFGHIJKLMNOPQRSTUVWXYZ

☐ CUSTOM ALPHANUMERIC ALPHABET

ABCDEFGHIJKLMNOPQRSTUVWXYZ012... x

► DECRYPT

Columnar Transposition Decode

Langkah terakhir masuk ke dcode.fr

Set:

Key: TRAFFIC
Mode: Decrypt

Search for a tool

★ SEARCH A TOOL ON dCODE

★ BROWSE THE [FULL dCODE TOOLS' LIST](#)

Results

BELAJARMACAMMACAMKRIPTOKLASIKXXXXXXXX

Columnar Transposition Cipher - [dCode](#)

Tag(s) : Transposition Cipher

Share

dCode and more

dCode is free and its tools are a valuable help in games, maths, geocaching, puzzles and problems to solve

Cryptography > Transposition Cipher > Columnar

COLUMNAR TRANSPOSITION DECODER

★ COLUMNAR TRANSPOSITION CIPHERTEXT

LCMKXRAPIXAAKLXJMRAXAMISXEAAOXBMTKX

★ KEEP SPACES, PUNCTUATION (AND OTHER CHARACTERS)

★ PLAINTEXT (PRESUMED) LANGUAGE English

DECRYPTION METHOD

☒ WITH THE ENCRYPTION KEY OR PERMUTATION

→ (3,7,4,5,6,2,1) ⇒ (7,6,1,...

☐ TRY SOME PERMUTATIONS (BRUTEFORCE UP TO SIZE 10)

GRID WRITING/READING ENCRYPTION DIRECTION

★ MODE Write by rows, read by columns (by default)

▶ DECRYPT

See also: [Caesar Box Cipher](#)

Boom. Keluar plaintext final:

BELAJARMACAMMACAMKRIPTOKLASIKXXXXXXXX

XXXXXXXX adalah padding block, abaikan.

Final Flag

FORESTY{BELAJAR_MACAM_MACAM_KRIPTO_KLASIK}