

Operation Forestry

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_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:** [11 11]
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 tambahin 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:  
ABCDEFGHIJKLMNPQRSTUVWXYZ
```

Masih unreadable: FSVKTZTNEOXMSWUCWADROLZMTMXMAEYZQWFJ

Vigenère Decode

Set mode decrypt, bagian key masukin HASH.

Masih unreadable: YSDDMZBGXOFFLWCVPALKHLHFMMFFTECSJWNC

Affine Decode

Affine di CyberChef langsung set:

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

Masih unreadable: PNIILYQJGDAACXZOMHCTSCSALLAAWRZNKXUZ

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.

The screenshot shows two adjacent web pages from dCode. The left page is a general search tool for various ciphers, with a specific section for the Hill Cipher. It displays the ciphertext "PNIILYQJGDAACXZOMHCTSCSALLAARZNKXUZ" and a 2x2 matrix input field containing "7", "8", "11", and "11". The right page is a specialized "HILL DECODER" tool. It has a "HILL CIPHERTEXT" input field with the same ciphertext. Below it is a section titled "I KNOW THE NxN MATRIX NUMBERS/VALUES" with a 2x2 matrix input field containing "7", "8", "11", and "11". To the right of this matrix are buttons for "RESIZE", "CLEAR", "FILL WITH 0", and "FILL WITH 1". A list of options for the matrix is shown below, with the "I KNOW THE NxN MATRIX NUMBERS/VALUES" option selected. Other options include "TRY/BRUTEFORCE ALL 2x2 MATRIX (VALUES < 10 + LATIN ALPHABET)" and various alphabet definitions (26 letters, 27 characters, etc.). At the bottom right is a "DECRYPT" button.

Columnar Transposition Decode

Langkah terakhir masuk ke dcode.fr

Set:

Key: TRAFFIC
Mode: Decrypt

Search for a tool

SEARCH A TOOL ON dCODE

e.g. type 'random'

BROWSE THE FULL dCODE TOOLS' LIST

Results

BELAJARMACAMMACAMKRIPTOKLASIKXXXXXX

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

LCMKXRAPIXAAKLXJMRAKAMISXEAAOBMCTKX

★ KEEP SPACES, PUNCTUATION (AND OTHER CHARACTERS)

★ PLAINTEXT (PRESUMED) LANGUAGE English

DECRIPTION METHOD

WITH THE ENCRYPTION KEY OR PERMUTATION
T R A F F ... → (3,7,4,5,6,2,1) ↪ (7,6,1,2,5,4,3,8)

TRY SOME PERMUTATIONS (BRUTEFORCE UP TO SIZE)

GRID WRITING/READING ENCRYPTION DIRECTIONS

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

► DECRYPT

See also: [Caesar Box Cipher](#)

Boom. Keluar plaintext final:

BELAJARMACAMMACAMKRIPTOKLASIKXXXXXX

XXXXXX adalah padding block, abaikan.

Final Flag

FORESTY{BELAJAR_MACAM_MACAM_KRIPTO_KLASIK}