

Operation Forestry

Player: Constantine

Kategori: Cryptography / Classical Stack

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

Konteks Dikit

Chall ini ngemix 6 lapisan kriptografi klasik yang dibungkus jadi satu ciphertext panjang.

Kita diberikan ciphertext:

GAHQCMCVFWJUAIDEISRZWTMUCUJUSFDMYIGP

Dan clue-clue dari buku catatan FORESTY yang secara eksplisit ngasih tau tiap layer cipher beserta parameternya.

Phase 1: Recon

Sebelum terjun ke tooling, kita identifikasi dulu urutan cipher saat enkripsi:

1. Columnar Transposition — key: **TRAFFIC**
2. Hill Cipher 2×2 — matrix: [7 8; 11 11]
3. Affine Cipher — $a = 3$, $b = 5$
4. Vigenère — key: **HASH**
5. Substitution — custom alphabet from **FORESTY**
6. ROT13 — final outer layer

Untuk decrypt, kita balik urutan:

ROT13 → Custom Substitution → Vigenère (decrypt) → Affine (decrypt) → Hill (decrypt) → Columnar (decrypt)

Di sini aku pakai CyberChef untuk layer 1–4, lalu dcode.fr untuk Hill & Columnar karena di CyberChef enggak ada.

Input: GAHQCMCVFWJUAIDEISRZWTMUCUJUSFDMYIGP

Output: PNIILYQJGDAACXZOMHCTSCSALLAWRZNKXUZ

Phase 2: Layer-by-Layer Execution

ROT13

Layer paling gampang. 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: FORESTYABCDGHijklmnPQUVWXZ

Di CyberChef:

Substitute → From: FORESTYABCDGHIJKLMNOPQUVWXZ → To:
ABCDEFGHIJKLMNOPQRSTUVWXYZ

Masih unreadable: FSVKTZTNEOXMSWUCWADROLZMTMXMAEUZQWFJ

Vigenère Decode

Set mode decrypt, bagian key masukin HASH.

Masih unreadable: YSDDMZBGXOFFLWCVPALKHLHFMMFFTECSJWNC

Affine Decode — a=3, b=5

Affine di CyberChef langsung set:

a = 3
b = 5
mode = Decrypt

Masih unreadable: PNIILYQJGDAACXZOMHCTSCSALLAWRZNKXUZ

Hill Cipher Decrypt — Matrix 2×2

Matrix dari clue:

7 8
11 11

CyberChef kadang gapunya di bagian ini, jadi aku pindah ke [dcode.fr](https://dcode.fr/hill-cipher) - Hill Cipher.

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

HILL DECODER

HILL CIPHERTEXT

PNIILYQJGDAACXZOMHCTSCSALLAAWRZNKXUZ

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

I KNOW THE NxN MATRIX NUMBERS/VALUES

7	8	: 2 <input type="button" value="▲"/> x .. <input type="button" value="▼"/> 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

ABCDEF...

Columnar Transposition Decode — Key: TRAFFIC

Langkah terakhir: masuk ke [dcode.fr - Columnar Transposition](https://dcode.fr/columnar-transposition).

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) ↪ (7,6,1,5,4,3,2,0)

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.

Phase 3: Recovery

Remove padding → format ulang sesuai rules.

Final plaintext:

BELAJAR MACAM MACAM KRIPTO KLASIK

Flag format: FORESTY{x_x_x_x_x}

→ Jadi:

FORESTY{BELAJAR_MACAM_MACAM_KRIPTO_KLASIK}