Operation Foresty

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

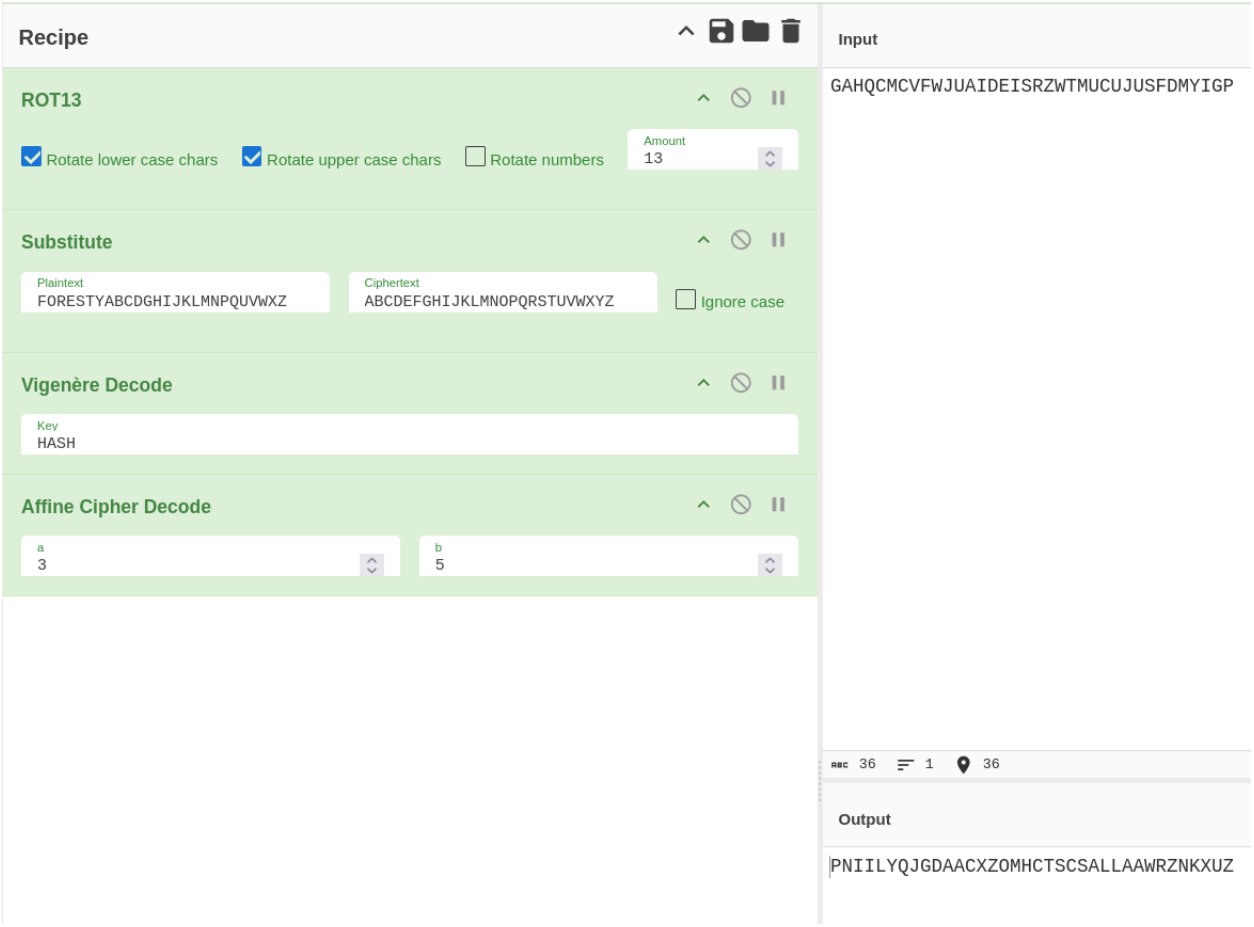
Sebelum terjun ke tooling, kita identifikasi dulu urutan cipher saat enkripsi:

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.



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: FORESTYABCDGHIJKLMNPQUVWXZ → 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: PNIILYQJGDAACXZOMHCTSCSALLAAWRZNKXUZ

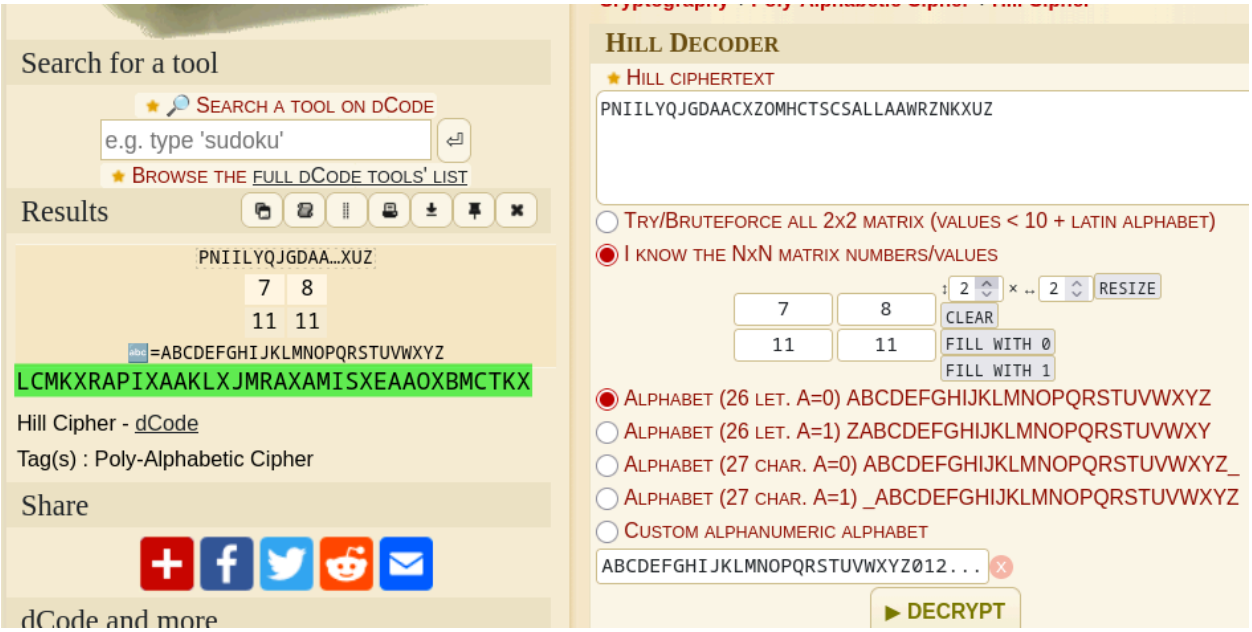
Hill Cipher Decrypt — Matrix 2×2

Matrix dari clue:

7 8
11 11

CyberChef kadang gapunya di bagian ini, jadi aku pindah ke **dcode.fr - Hill Cipher**.

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



Columnar Transposition Decode — Key: TRAFFIC

Langkah terakhir: masuk ke **dcode.fr - Columnar Transposition**.

Set:

Key: TRAFFIC
Mode: Decrypt

Boom. Keluar plaintext final:

BELAJARMACAMMACAMKRIPTOKLASIKXXXXXXX

XXXXXXX 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}