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_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 2×2** - `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: 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

Affine di CyberChef langsung set:

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

Masih unreadable: PNIILYQJGDAACXZOMHCTSCSALLAAWRZNKXUZ

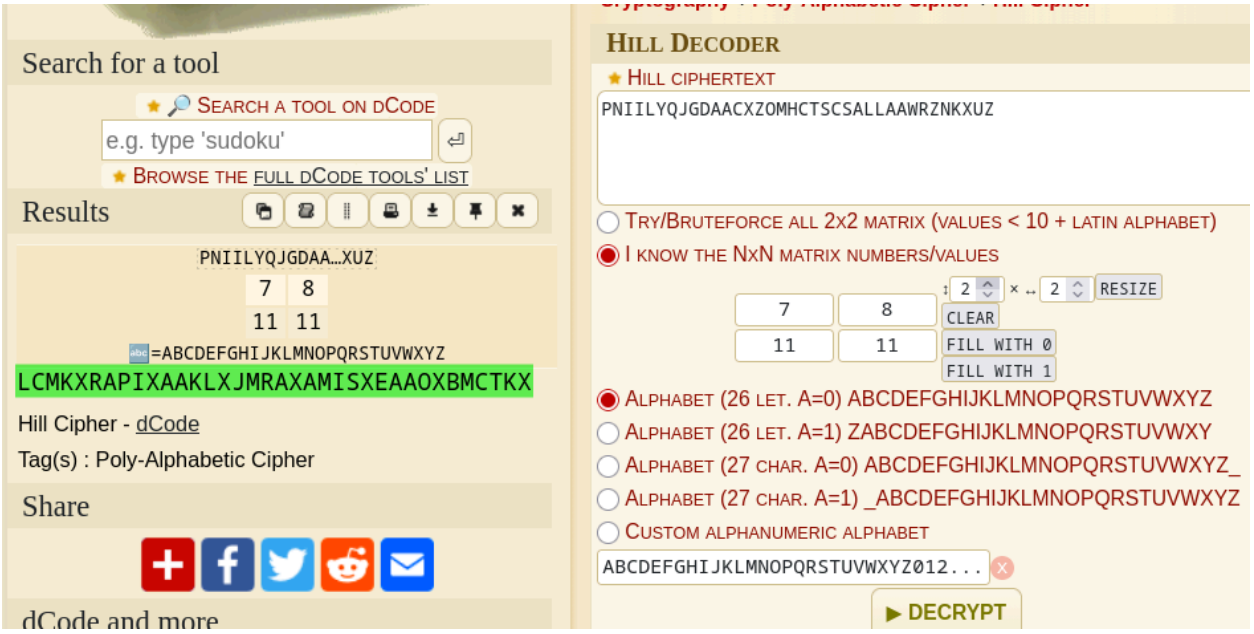
Hill Cipher Decrypt

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.



Columnar Transposition Decode

Langkah terakhir masuk ke dcode.fr

Set:

```
Key: TRAFFIC
Mode: Decrypt
```

Boom. Keluar plaintext final:

BELAJARMACAMMACAMKRIPTOKLASIKXXXXXXX

XXXXXXX adalah padding block, abaikan.

Final Flag

FORESTY{BELAJAR_MACAM_MACAM_KRIPTO_KLASIK}