# As If It’s Your Last Shared Secure Key

An encrypted flag has been intercepted. Your mission: recover the hidden plaintext.
Captured data:

```
{
"ciphertext": "NOCh+xPquuXcrhHL5NjHmxYqjaNzwtG7",
"iv": "gi6GBRjZcNBaOAC/",
"tag": "Gw4cfuFEpdMWa7zVoNbtDg=="
}
```

The system hosting the flag is running at:
https://asif.cyberbattle.info

## Recon

The service exposes three vulnerable endpoints:

### 1. /ecdh/generate-keys-and-encrypt

Spin up your own ECDH keypair and encrypt a chosen message.
Example:

```
POST /ecdh/generate-keys-and-encrypt
{
"message": "PLAINTEXT_TO_BE_ENCRYPTED"
}
```

### 2. /ecdh/shared-secret-key

Combine a private key with a peer’s public key to forge the shared AES key.
Example:

```
POST /ecdh/shared-secret-key
{
"privateKey": "INSERT_PRIVATE_KEY_HERE",
"publicKey": "INSERT_PUBLIC_KEY_HERE"
}
```

### 3. /ecdh/decrypt

Use the derived AES key to break open a ciphertext.
Example:

```
POST /ecdh/decrypt
{
"ciphertext": "INSERT_CIPHERTEXT_HERE",
"iv": "INSERT_IV_HERE",
"tag": "INSERT_TAG_HERE",
"aesKey": "INSERT_AES_KEY_HERE"
```

}

## Objective

- Investigate how the system handles your chosen messages.
- Craft the correct shared AES key using the provided public data.
- Use that key to decrypt the intercepted ciphertext.
- The plaintext you recover is the flag.

## Hint

Encrypt your own test messages first. The patterns you observe will reveal the path to the flag.