CTF 101: ROP the Flag

Introduction to Cryptography

By RoyalRoppers

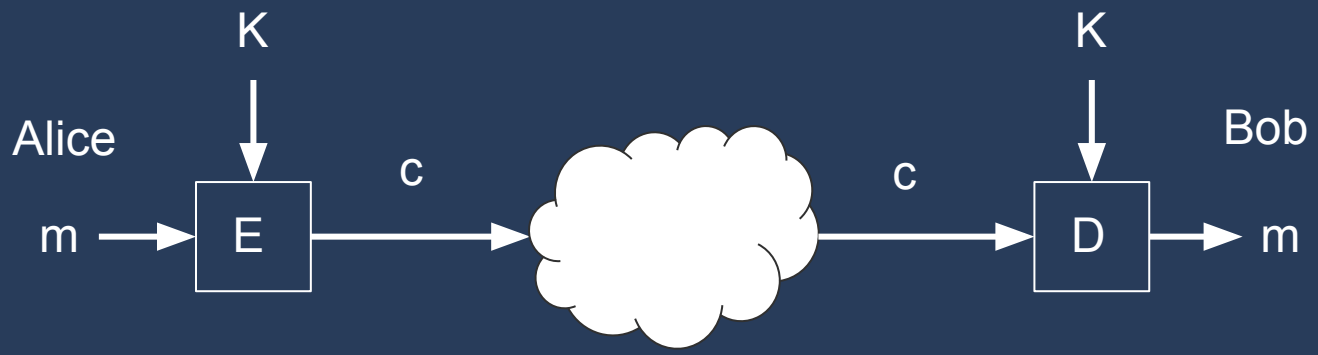

FOI
Crate-CTF
2025
FÖRSVARSMAKTEN
foi.se/cratectf

Cryptography (Crypto)

- Decoding or breaking encryption methods
- Classical Ciphers - Caesar, Vigenère, Substitution, etc.
- Modern - RSA, AES, ECC, etc.
- Hash Functions - MD5, SHA-256, etc.
- Useful tools:
  - SageMath
  - SymPy
  - dcode.fr
  - CyberChef

Example: EblnyEbccref → (Rot 13) → RoyalRoppers

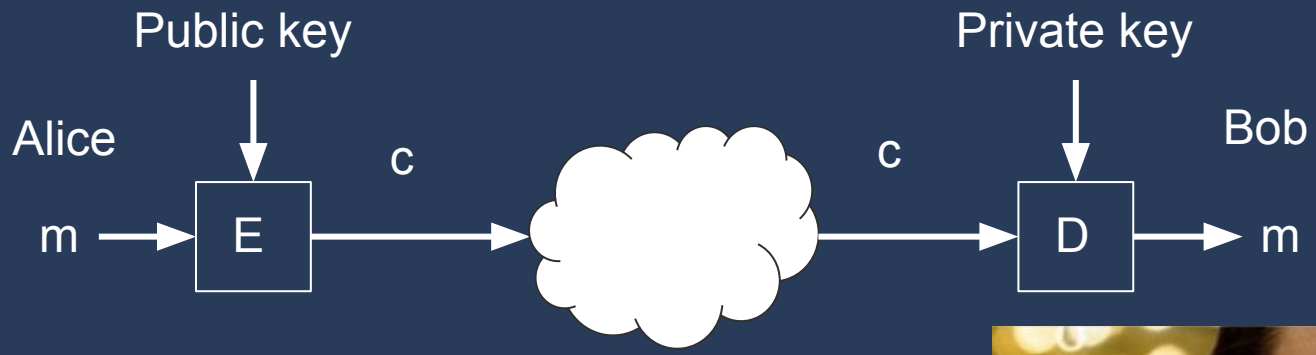
Symmetric Crypto



Example:

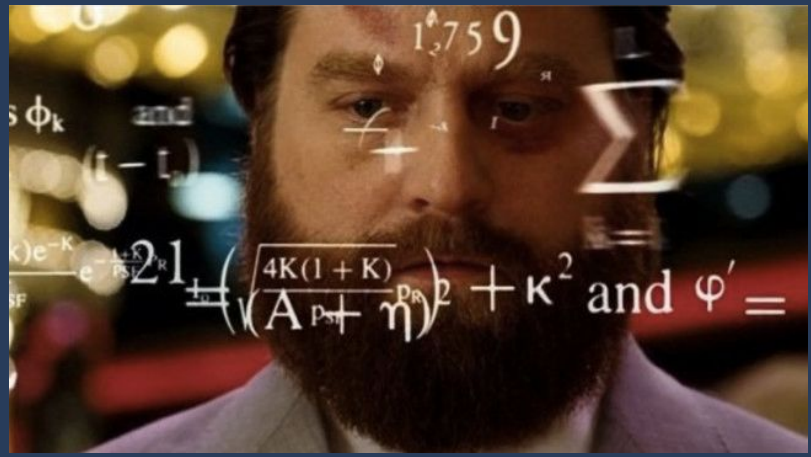
- Classic ciphers
- AES
- DES
- Blowfish
- RC4
- Salsa20

Asymmetric/Public Key Crypto



Example:

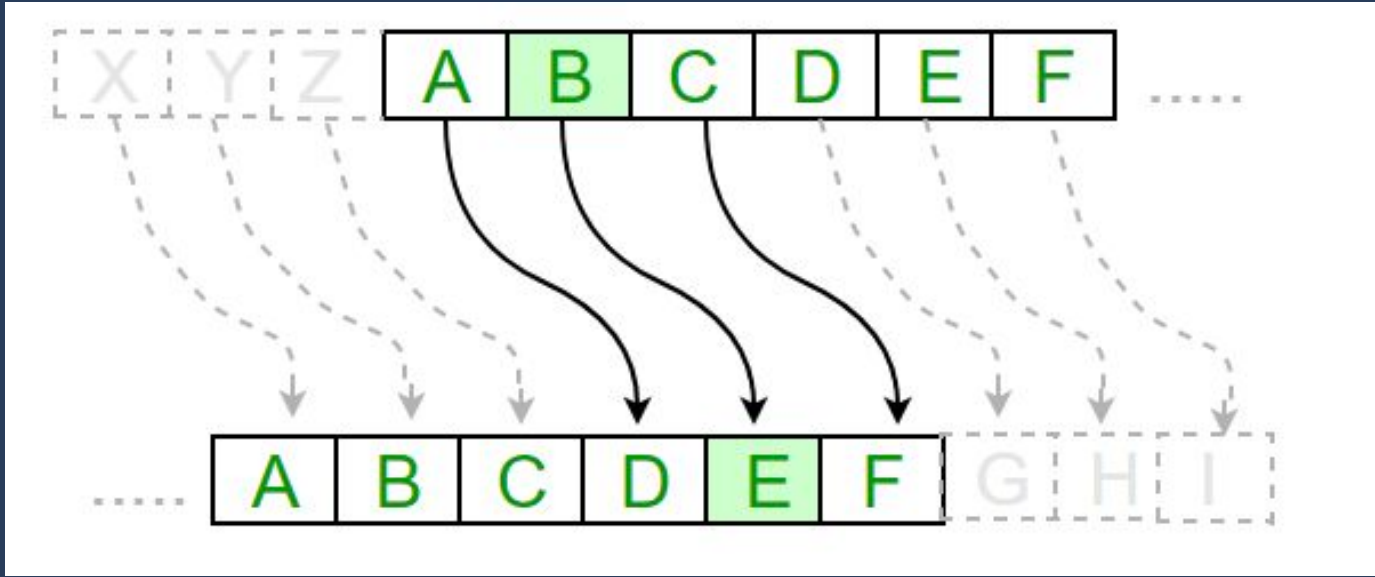
- RSA
- Diffie-Hellman
- ElGammal
- Elliptic-curve cryptography (ECC)



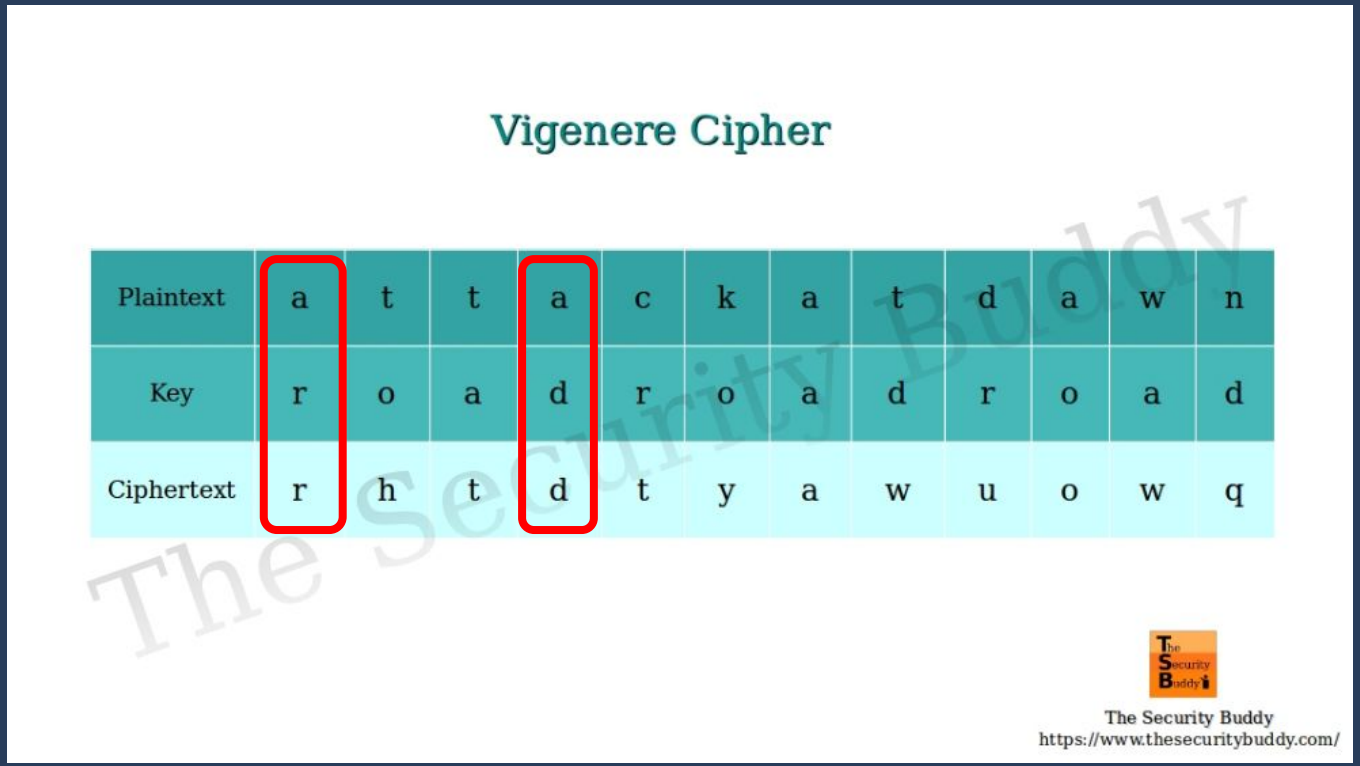
Caeser Cipher

$$E(m) = m + k \mod 26$$

$$D(c) = c - k \mod 26$$



Vigenère Cipher



XOR

- Exclusive or: ^ ⊕

Truth table	0	1
0	0	1
1	1	0

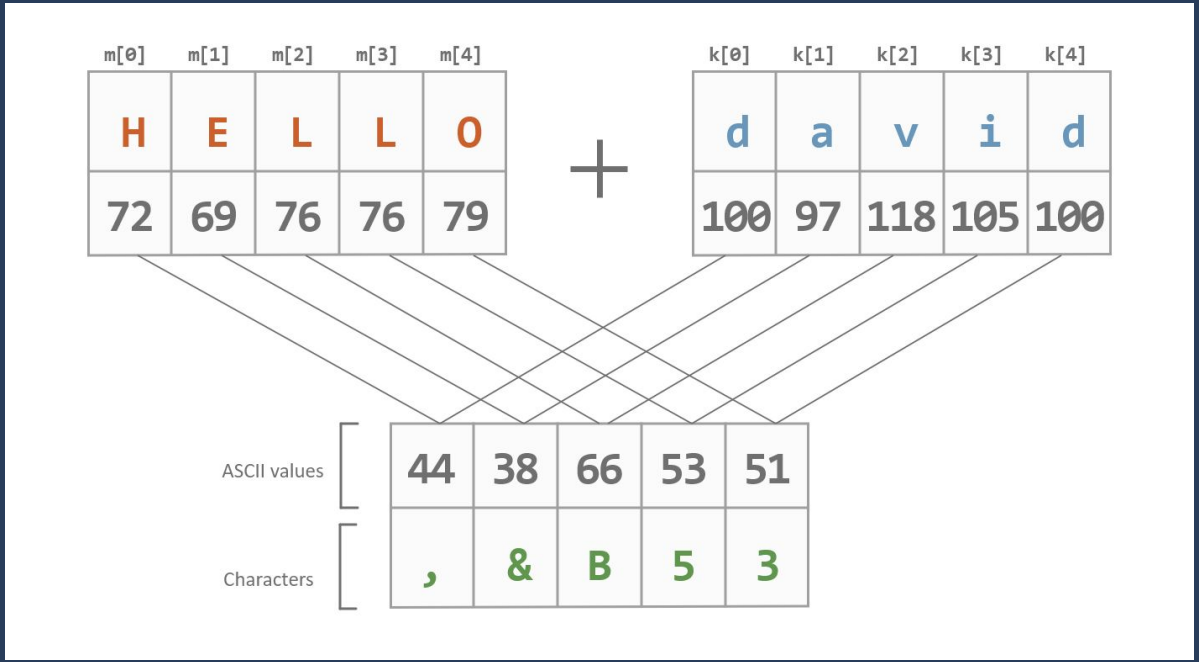
6 = 110
3 = 011

6^3 = 101

- x ^ x = 0
- x ^ 0 = x

One-time pad

- Message (n bits): m
- Random key (n bits): k
- c = E(m) = m ^ k
- m = D(c) = c ^ k
- Totally secure!



RSA

- Randomly select two large prime numbers **p** and **q**
- Calculate **N = p * q**
- Calculate **phi(N) = (p-1) * (q-1)**
- Select e such that p-1 and q-1 are relatively prime to e. Same as if phi(N) and e are relatively prime
- Calculate **d** from **ed = 1 (mod phi(N))**

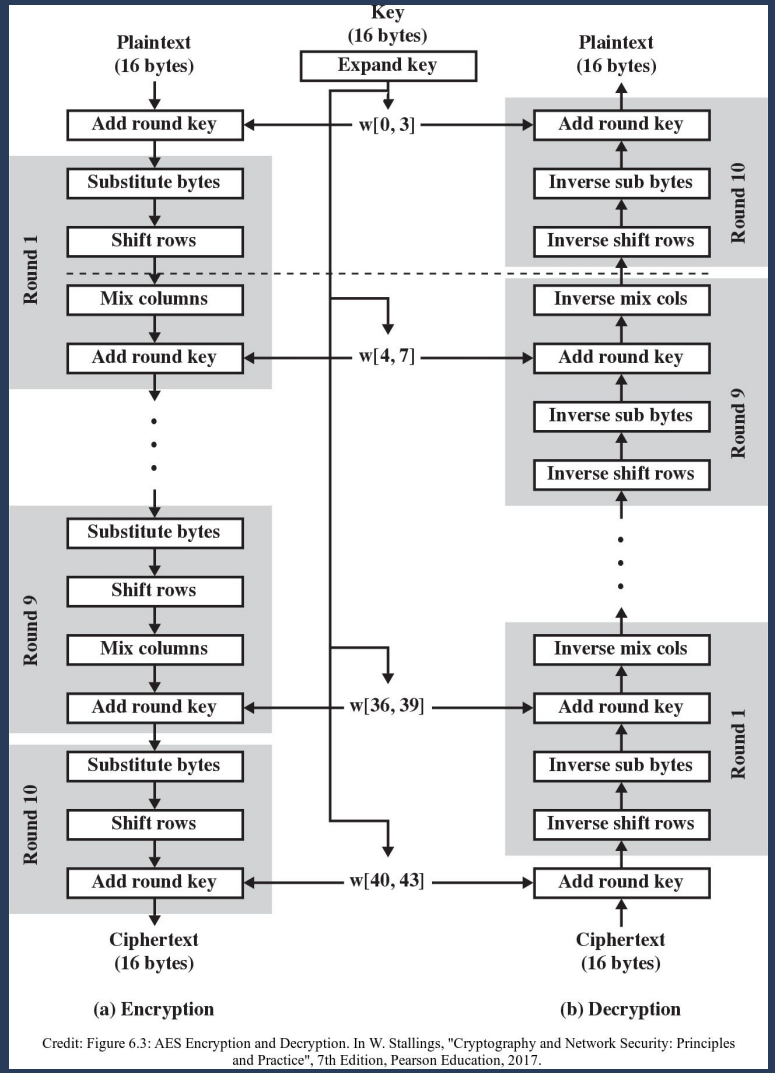
Encryption: $m^e = c \pmod N$
Decryption: $c^d = (m^e)^d = m^{(e*d)} = m^1 = m \pmod N$

What can go wrong with RSA?

- Primes are too small
- Primes are too close to each other
- m and e are too small for a large public key
- Reuse of N = pq with different e
- p == q
- dq and dp “leaked”
- Small private key d → Wiener’s attack
- Power trace attacks
- …

AES

Cool shit!

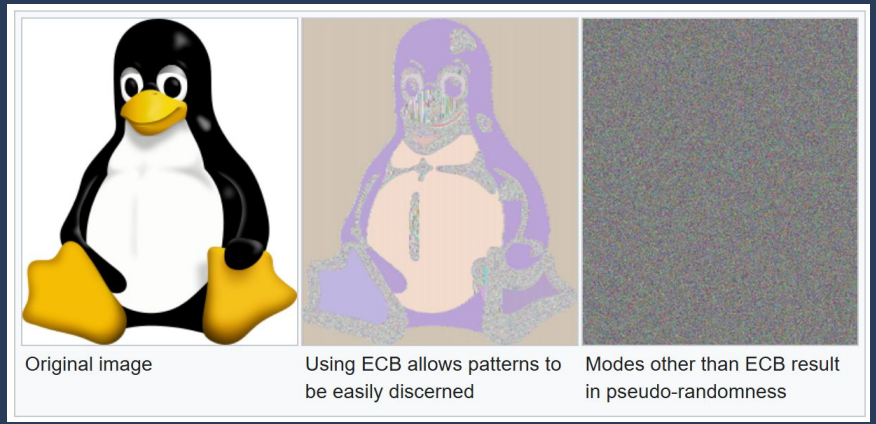


Credit: Figure 6.3: AES Encryption and Decryption. In W. Stallings, "Cryptography and Network Security: Principles and Practice", 7th Edition, Pearson Education, 2017.

What can go wrong with AES?

Mostly wrong use of AES modes:

- ECB
  - Look at the picture
  - AES-ECB Padding
- CBC
  - Padding Oracle
  - Bit Flipping
- CTR
  - IV reuse
- GCM
  - Nonce reuse
- Cache side channels

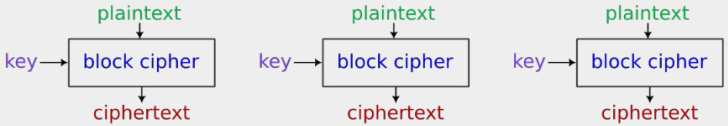


Original image

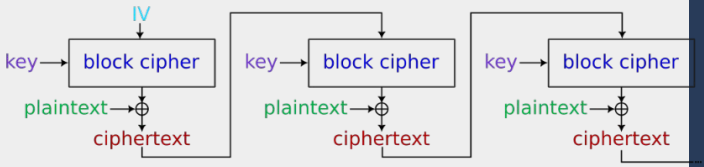
Using ECB allows patterns to be easily discerned

Modes other than ECB result in pseudo-randomness

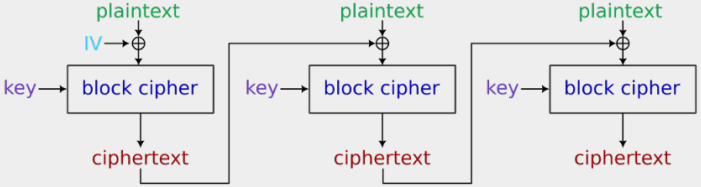
Electronic codebook (ECB)



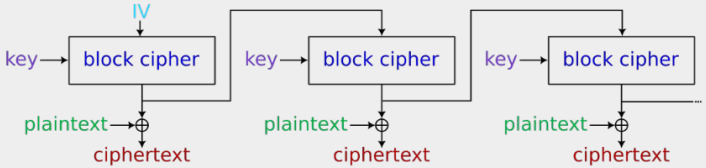
Cipher feedback (CFB)



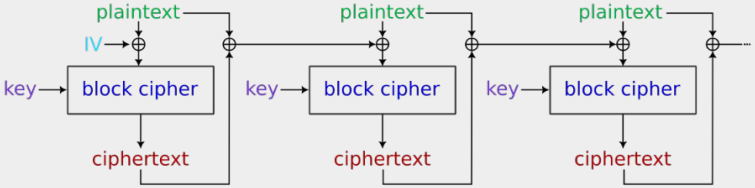
Cipher block chaining (CBC)



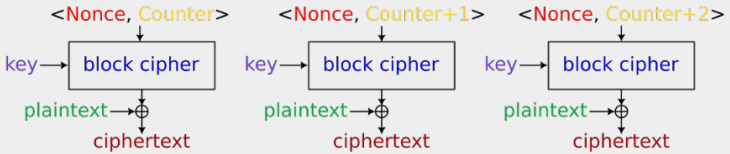
Output feedback (OFB)



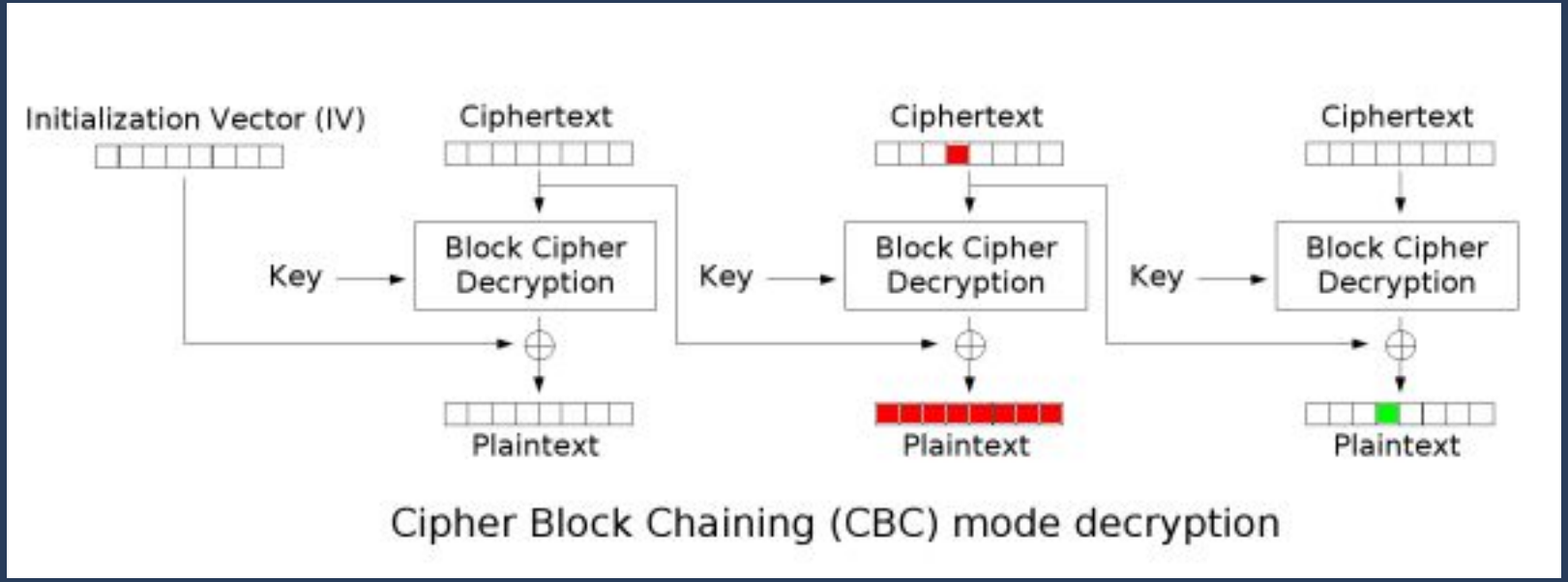
Propagating cipher block chaining (PCBC)



Counter (CTR)



CBC Bit-Flipping Attack



A lot more cryptography

- Classical ciphers like Caesar
- DES or ChaCha20
- ECC (Elliptic Curve Cryptography)
- Hash algorithms such as MD5 or SHA1
- Lattice-based cryptography
- Custom ciphers

Challenges!!!

Credits

- Nullcon Goa HackIM 2025 CTF
- LA CTF 2025
- UIUCTF 2017

Links

- SSM
- CryptoHack
- cryptopals
- Own collection of some challenges (without solutions)
- Own collection of some challenges (with solutions)