

ark1nar Yubitsec CTF - Write Up Crypto Latest commit af115e3 2 days ago

..

| | | |
|---|---|---|
| src/RSA | Yubitsec CTF - Write Up Crypto | 2 days ago |
| readme.md | Yubitsec CTF - Write Up Crypto | 2 days ago |

readme.md

RSA 1 - Crypto - 325

Enoncé :

```
Can you decrypt these ciphertexts ?
```

Sources

Résolution :

Même chose pour les 3 clés :

On récupère les informations contenues dans la clé publique :

```
openssl rsa -in pubkey.pem -pubin -text -modulus
```

On remarque que le modulo est faible :

```
Public-Key: (149 bit)
Modulus:
    1a:ac:d3:c9:0d:1a:bd:fd:dd:de:18:35:f5:8a:88:
    f0:36:8b:9f
Exponent: 65537 (0x10001)
Modulus=1AACD3C90D1ABDFDDDDE1835F58A88F0368B9F
-----BEGIN PUBLIC KEY-----
MC4wDQYJKoZIhvcNAQEBBQADHQAwGgITGqzTyQ0avf3d3hg19YqI8DaLnwIDAQAB
-----END PUBLIC KEY-----
Public-Key: (154 bit)
Modulus:
    03:8a:f3:1e:59:8e:24:2b:5f:cf:1b:30:6f:df:f0:
    e2:d6:6e:f2:39
Exponent: 65537 (0x10001)
Modulus=38AF31E598E242B5FCF1B306FDFF0E2D66EF239
-----BEGIN PUBLIC KEY-----
MC8wDQYJKoZIhvcNAQEBBQADHgAwGwIUA4rzHlmOJCtfzxswb9/w4tZu8jkCAwEA
AQ==
-----END PUBLIC KEY-----
Public-Key: (151 bit)
Modulus:
    65:7a:90:84:26:10:1a:fa:25:51:cf:ca:26:e3:9a:
    f5:64:53:27
Exponent: 65537 (0x10001)
Modulus=657A908426101AFA2551CFCA26E39AF5645327
-----BEGIN PUBLIC KEY-----
MC4wDQYJKoZIhvcNAQEBBQADHQAwGgITZXqQhCYQGvolUc/KJuOa9WRTJwIDAQAB
-----END PUBLIC KEY-----
```

On passe le modulo de hexa à int est on le factorise :

```
sage : n=int("mon_modulo_en_hexa",16)
sage : factor(n)
```

On récupère p & q on recréé les clé publique avec rsatool :

```
python rsatool.py -p mon_p -q mon_q -f PEM -o privkey.pem
```

On déchiffre :

```
openssl rsautl -decrypt -inkey privkey.pem -in cipher.txt
```

flag : YUBITSEC{S4V3_FL46}

By team Beers4Flags