nexenio

Hacking Adventures

Preparation

- https://github.com/neXenio/hacking-adventures
  - python/challenge-4
- Install Python 3.8+
  - either locally
  - or use https://jupyter.org/try-jupyter/lab/

Goal for Today

- Crack RSA
- Decipher the following texts
  - 733f71c920072be41d6c6f416686e63f
    84133f18b7f683a85a975f6b94fb2798
    3012aff76f1633ddc01bd8942c793acd
  - 5232ceca3cca9d575fa5744d429ca945
    34729a4e9ae525c83d58f97f1204be6c
    5402a9076cfcd525e204ca81de13672d
    6cfd8660758727a4d0f7e39901377c96
    2dcad4d39a287b1565401078626 3be11

RSA Basics

- Integer factorization is hard, e.g.
  - 91 = … ?
  - 8051 = … ?
  - 66609645572837301 19 = … ?

RSA Basics

- Integer factorization is hard, e.g.
  - 91 = 7 × 13
  - 8051 = … ?
  - 66609645572837301 19 = … ?

RSA Basics

- Integer factorization is hard, e.g.
  - $91 = 7 \times 13$
  - $8051 = \underline{\mathbf{8100 - 49}} = 90^2 - 7^2 = (90 - 7) \times (90 + 7) = 83 \times 97$
  - 666096455728373011 9 = … ?

RSA Basics

- RSA Key Pair based on 8051 = 83 × 97
  - p = 83, q = 97, n = 8051
  - φ = (p-1) × (q-1) = 7872
  - e = 5
  - d = e^{-1} mod φ = 3149 (3149 × 5 = 15745 = 7872 × 2 + 1)
  - encryption → public key = (e, n) = (5, 8051)
  - decryption → secret key = (d, n) = (3149, 8051)

RSA Encryption

- encryption → public key = (e, n) = (5, 8051)
- Text = “Hello” → 48 65 6C 6C 6F (hex) → 72 101 108 108 111 (dec)
  - enc(72) = **$\underline{72^{e} \bmod n}$** = $72^{5} \bmod 8051 = 4700 = 125C$
  - …
  - enc(111) = $111^{5} \bmod 8051 = 7622 = 1DC6$
- enc(“Hello”) = 125C BF5 118D 118D 1DC6

RSA Decryption

- decryption → secret key = (d, n) = (3149, 8051)
- ciphertext 125C BF5 118D 118D 1DC6 (hex) → 4700 3061 4493 4493 7622 (dec)
  - dec(4700) = **$\underline{4700^{d} \bmod n}$** = $4700^{3149} \bmod 8051 = 72$
  - …
  - dec(7622) = $7622^{3149} \bmod 8051 = 111$
- dec(125C BF5 118D 118D 1DC6) = 72 101 108 108 111 → “Hello”