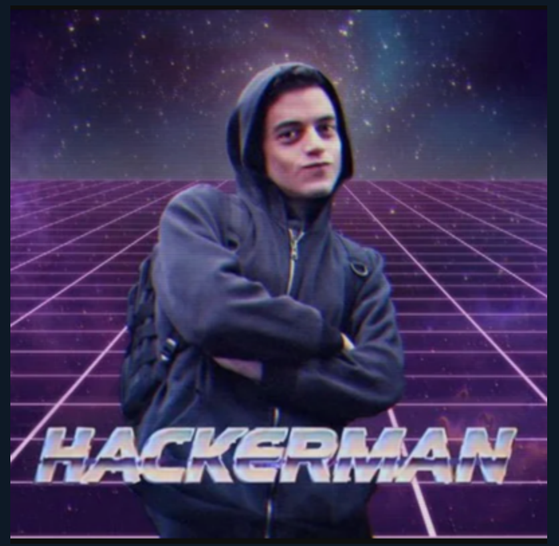
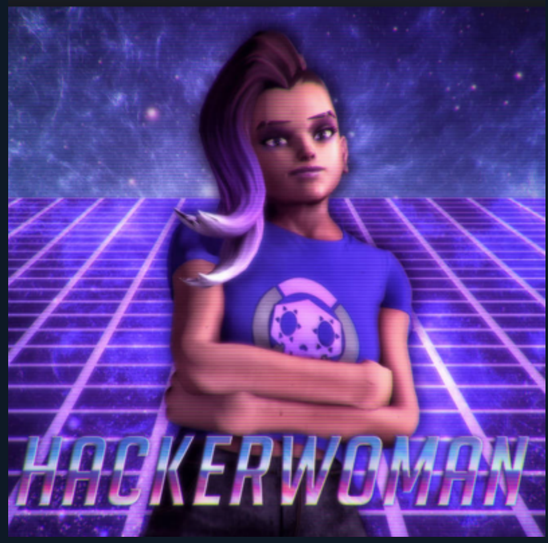
nexenio

Hacking Adventures

Motivation

- Hacking is for everyone!
- “How can I break this?” vs.
  “How do I get this to work?”
- Obviously no bugs vs.
  No obvious bugs
- It takes one to know one





Preparation

- https://github.com/neXenio/hacking-adventures

- Branches:
  - kotlin/challenge-1
  - swift/challenge-1
  - python/challenge-1
  - js/challenge-1

- DM me about pair programming partner and other languages

Some Myths

- Total security
  - security isn’t binary, think instead about decreasing the risk of a breach
- You need to have expert knowledge
  - awareness of social engineering (e.g. phishing) is already great
- It’s not your job
  - … until you need to update your dependencies

Goal for Today

- Decrypt the following ciphertexts
  - 1b373733313363f78151b7f2b7834313333d78397828372d363c78373e783a393b3736
  - ZNKIGKYGXIOVNKXOYGXKGRREURJIOVNKXCNOINOYXKGRRECKGQOSTUZYAXKNUCURJHKIGAYKOSZUURGFEZURUUQGZZNKCOQOVGMKGZZNKSUSKTZHAZOLOMAXKOZYMUZZUHKGZRKGYZROQKLOLZEEKGXYURJUXCNGZKBKXBGPJADLIVBAYKZNUYKRGYZZKTINGXGIZKXYGYZNKYURAZOUT
  - EANOEHHNFJLFXDGFANOYDJINTNOEDJXFOSBFESDOLGDWWSNUEDJNQCSJNUFEFFOUIDTTCOSIFESDOLNJKSINLEDNOXSONNJEZNSJMJDUCI…

Substitution via Shift

- Decrypt the following ciphertext
  - `URYYB JBEYQ UNYYB JRYG`
  - `HELLO WORLD HALLO WELT`

  - `NOPQRSTUVWXYZABCDEFGHIJKLM`
  - `ABCDEFGHIJKLMNOPQRSTUVWXYZ`

Substitution via XOR

- 0 ^ 0 = 0
  1 ^ 0 = 1
  0 ^ 1 = 1
  1 ^ 1 = 0
- ‘a’ ^ ‘?’ = 97 ^ 63 = 0b01100001 ^ 0b00111111
  = 0b01011110
  = 94
  = ‘^’
- ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz
  ~}|{zyxwvutsrqponmlkjihgfe^]\[ZYXWVUTSRQPONMLKJIHGFE

Hints

- base64 converter not yet relevant
- Challenge 1A is hex-encoded, plaintext is ASCII-encoded
- Challenge 1B and its plaintext are both ASCII-encoded
- Challenge 1C and its plaintext are both ASCII-encoded
- XOR-helper method expects same length inputs
- Challenge 1C is significantly more challenging and requires a statistical approach for common groups of letters (e.g. “tion”) - look up quadgrams