FM Hunting

Challenge Description

A remote service streams raw baseband IQ samples at 48 kHz over TCP. The signal is a simple 2-FSK beacon carrying a hidden payload.

1. IQ Capture

The IQ stream is captured directly from the socket:

```
nc 65.109.194.34 7356 > iq.bin
# mirror:
# nc 65.109.210.233 7356 > iq.bin
```

A capture length of roughly 60 seconds is required to recover the full transmitted payload.

2. FM / FSK Demodulation

The stream consists of interleaved signed I/Q samples. A quadrature FM discriminator is applied:

$$y[n] = \angle\left(x[n] \cdot x^*[n-1]\right)$$

This converts instantaneous frequency shifts into baseband amplitude, revealing a 2-FSK waveform.

3. Symbol Recovery

- Sample rate: 48 kHz
- Estimated symbol rate: 200 baud (via autocorrelation)
- Demodulation: integrate-and-dump
- Bit slicing: threshold at zero
- Bit order: LSB-first

A long 0x55 (‘‘U’’) preamble is visible, confirming correct symbol alignment.

4. Decoded Payload

After decoding the bitstream to bytes, readable ASCII appears:

```
BEGIN
This file contains a message encrypted with XOR.
Key address (byte offset) = 420
Flag address (byte offset) = 698
```

The transmitted data is treated as a file, where:

- XOR key starts at byte offset 420
- XOR-encrypted flag starts at byte offset 698

5. XOR Decryption

Bytes at offset 698 are XOR-decrypted using the key starting at offset 420 (repeating key). The decrypted plaintext yields the flag.

6. Flag

`ASIS{XOR_A11_7H3_7H1NG5}`

Conclusion

This challenge demonstrates a classic RF CTF workflow: IQ capture → FM discrimination → FSK slicing → ASCII decoding → XOR decryption.