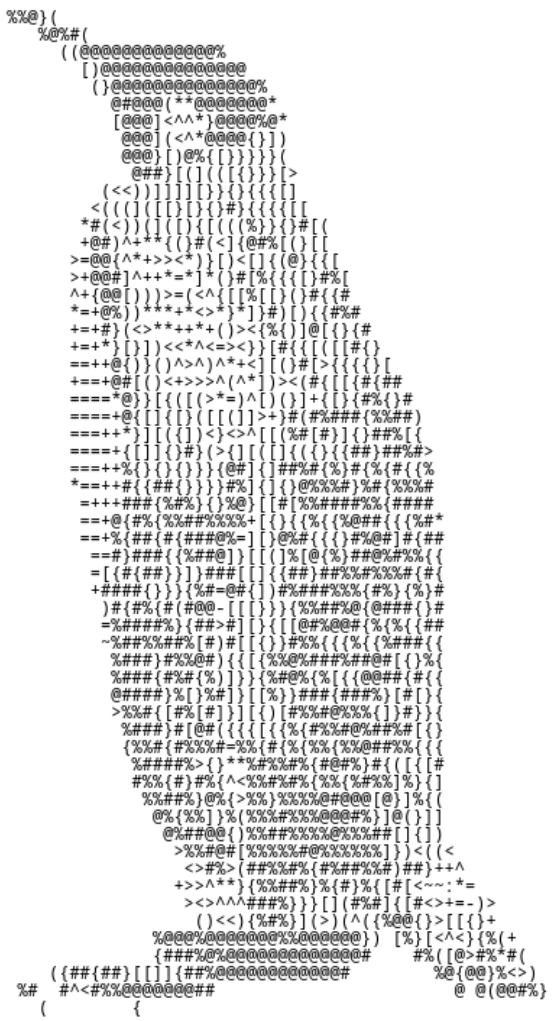
The Art of Frightful CTFs

By Matthew Townsend



This Document is a series of CTF challenges designed for those seeking higher challenges during a Hackathon event or overall performance. These have been curated through personal interest or group disgust as in the beginning challenge set.

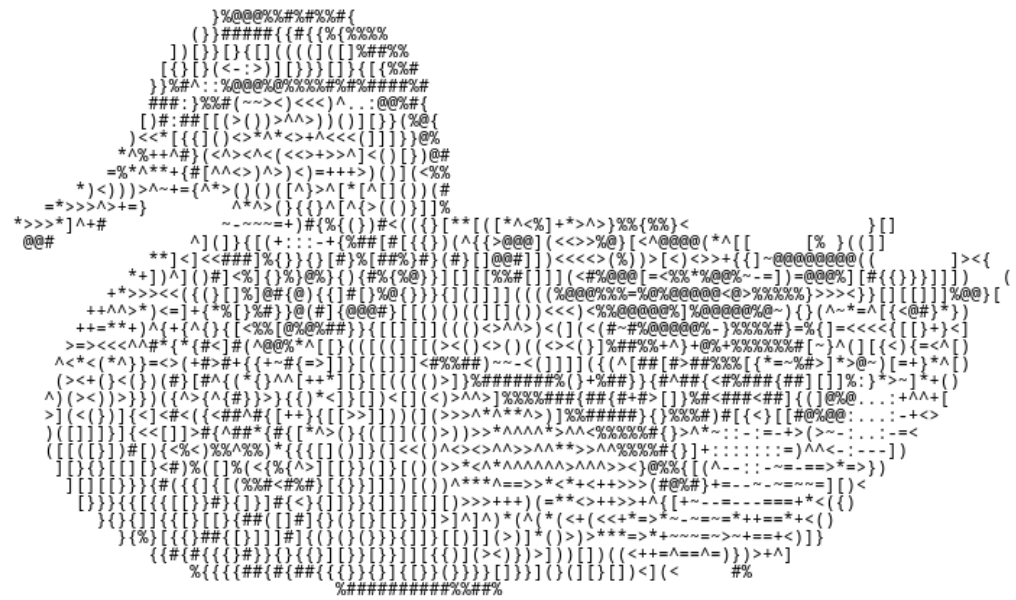
There is a subsequent GitHub repo linked for these challenges that can be found at the following address: https://github.com/M01010100/Matts_QDucks. It was aptly named, as I was going to leave this document at set one, but where's the fun in limiting the possibilities?

The topics will vary greatly but will keep themes to topics, ie, Quantum-Mystical, Crypto-Pirates (Crypto as in Cryptology), etc.

Index

Matt’s Quantum Ducks

By Matthew Townsend



I sought the challenge of quantum, the last difficult class to conquer at SUNY Poly. I now come to bear the weight of the knowledge unto you. Have fun, it could save your team, or destroy it.

_____

Preamble

As the Qubit Oracle, I bestow upon you the opportunity, if you accept, to earn a q-duck, which may be traded in for an additional 20% points for your team, or else ***if it*** is deemed so. The completion of each step earns you the right to provide the input to the Schrodinger's Wheel.

If you do accept, open the Pandora's box in the room. Only the brave will survive.

_____

Step 1 - XX Points:

Let's get those math brains going. Message M01010100 on Discord or ask for him in the room.

Compute the Inner Product of the vectors

(011101) and (110100)

|0110> and |1100>

- -

The Wheel of Fate

A custom-coded wheel that, if you choose to spin, may give great fortune or famine to the team.

Provide an input (00, 01, 10, 11)

- -

_____

Step 2: Intro to logic - XX Points:

Oh look the ducks have found themselves quantum logic gates, you should appease them for a chance to spin the wheel and points.

They found two Hadamard Gates and a Pauli-X gate, They insist that they equal a Pauli Z gate. You should prove it.

X - 01 H - $\frac{1}{\sqrt{2}}$ $\begin{matrix} 1 & 1 \\ 1 & -1 \end{matrix}$ Z: $\begin{matrix} 1 & 0 \\ 0 & -1 \end{matrix}$

10

Step 3: Crossed Streams - xx points

The ducks crossed their wakes and lost track of their path. Can you determine which duck belongs to the wires (A, B)

```
dev = qml.device("default.qubit", wires=["A", "B"])
@qml.qnode(dev)

def circuit(state):
    qml.Hadamard(wires="A")
    qml.CNOT(wires=["X", "B"])

    if(state[1] == 1):
        qml.X(wires="X")
    if(state[0] == 1):
        qml.Z(wires="X")

    qml.CNOT(wires=["X", "X"])
    qml.Hadamard(wires="X")

 return qml.state()

state = np.array([0, 1])
print(circuit(state))
_ = qml.draw_mpl(circuit, style="pennylane")(state)

###DESIRED OUTPUT
[0.+0.j 1.+0.j 0.+0.j 0.+0.j]
```

Step 4: The Q-duck - xx points

Now is the time to determine the fate of your feeble team; you can change your fate or cement it if you continue. This will be your time to code a simulated quantum circuit in pennylane.

Simulate a Quantum teleportation using Pennylane.

A Crypto Voyage

Are you ready to sail the seas of cryptology, from Caesar's reign to the publication of PGP? We will venture through the interesting quarrels and mathematical advancements.

Physical Challenge points - xx

Review historical early forms of cryptography and create a new method of hiding a message in plain site. This does not need to involve math, only ingenuity.

Ex: https://en.wikipedia.org/wiki/Cryptography#Classic_cryptography

---

Let's Start Easy: points - 10

1. What is the transaction ID for the infamous Bitcoin Pizza?
2.

Step 1 - easy - xx

Let's jump straight into action. It's 1941, and you've just intercepted this broadcast from a German bomber. Your mission is to decrypt this message.

uejh rtlb bbbc ndlf qxge i

1. Hint: After recovering the machine from a u-boat, you know the ring is 3c.
2. Hint: There is a second round of encryption, but is it the same or a ***ROMAN*** cipher?

Step 2 - Medium - xx

Let's jump ahead 40 years and we need to share our keys, lets use diffie hellman key exchange.

P = 3049
G = 2096
A = 960
B = 780

What is our secret ?