CTFAirways Unintended Solution

While troubleshooting deployment problems with the CTFAirways task, an unintended solution was discovered. This solution doesn't require code execution inside the AFDX network, it simply solves the task by using the throttled online service (0.5 qps).

This was an oversight while defining the limits of the task. It was assumed that the task took 5-10 minutes to solve at full CPU speed, but it turns out most of the time is spent waiting for the network, which means the number of required tests is significantly smaller than expected.

Assuming no parallelization, the only challenge players have to overcome is the correct decoding of the FDR data backups. These are in a predictable, although a bit annoying, order. This allows players to bypass the RCE stage of the task.

Solving the proposed flag requires 5,000 requests, and the challenge limits players to 1 request every 2 seconds, so solving the task would take 10,000 seconds, which is roughly equivalent to 3 hours. Originally it was thought the number of requests was one order of magnitude higher (over 24 hours). The flag given to players as an example is 6 times harder, so it would take 18 hours to solve using this technique (originally thought to be around 200 hours).

It was assumed players taking this approach would compensate with parallelization, which is an acceptable path to a solution, although a bit harder to code. It turns out parallelization isn't necessary at all, which **makes the solution path of skipping the RCE somewhat acceptable**.

Solving the lights problem alone, requires noticing that each bit can be brute forced independently, and creating an algorithm that allows for brute forcing within the constraints of the key. This stage of the task is equally difficult for everyone.

Ordering the FDR backups and implementing parallelization adds some difficulty to the task in the form of work required to solve it. Teams that solve the task with RCE don't have to worry about this. On the other hand, gaining RCE in the task is easy, but troubleshooting it might be difficult. Teams that solve the task without RCE don't have to worry about this.

Overall, the difficulty of the challenge means that one of the paths to the solution is easier than the RCE. Since it takes around 3 hours, even without parallelization, it means players will likely have enough time to do multiple attempts, even if they have small coding errors.

Overall difficulty:

- Discovery is likely to be around 30 minutes to 1 hour
    - Read all documents, and review all relevant code.
- Research is likely to take between 4-6 hours (down from 8 hours)
    - Solve the CDLS circuit problem and code it locally.
- Exploitation is likely to be around 4-6 hours (down from 12 hours)
    - Troubleshoot and execute remotely.