My Game - Crypto (400? idk)

Letters intertwined

The end, recombined.

Awake, lying blinking,

Intensely thinking.

Muse and proclaim...

“It’s my game!”

?HLJ1>AA"AII>888!CE9>AA>"~>IIG888BAA~@>d>B~B?HH0bAI>>AE&>IIAACMQa

My Game (Solution)

The first letters of the flavor text spell out LITERALBITMAPIMG (Literal bitmap img). Using this information, they should be able to reconstruct an image which contains the flag **RC3-2016-JAIP3GEZ**.

jayp3gez.png

Agent G - Crypto 500

Agent G: We have a mission for you. The fate of the nation could very depend on your assistance! These channels are not secure; if you wish to accept the mission you must first find our more secure transmission.

[Add a link / embed the image from 1 - Image Stego]

Agent G (Solution)

I've attached 2 zips. One has the raw challenge materials and resources for solving / creating the challenges. The other has the flask webapp necessary to run the server portion of this challenge. The flag is **RC3-2016-J.BOZART**.

The text file crypto 500 has more detail about the solution to this challenge but here is a high level overview:

1. Image stego using steghide
   1. The key hint is in the metadata ("kHZ?") Key is 4625
   2. Image has payload rot47 encoded
2. Navajo code talkers
   1. Alphabet based on table here: <https://en.wikipedia.org/wiki/Code_talker#Navajo_code_talkers> and list of navajo numbers 2-7
   2. Navajo payload is base32 encoded
3. Morse code / Spectrogram
   1. Server plays morse code on loop
   2. Distortions in morse code caused by Coagula to embed image data into the waveform
   3. xoring the morse code and the hex bytes from the spectrogram results in the final plaintext
   4. FYI There are 10 segments of morse code, however the server requests should look like they're random and form a continuous stream. The first segment played is likely not segment 0 in the stream, but proper decoding should make it pretty clear where the real start is. The tracks are guaranteed to be in order.
4. Book Cipher based on Playlist
   1. The first song is the "key". it's basically a numbers station, the only lyrics are 0096 2251 2110 8105. These are used as 0-based indices into the songs in the rest of the playlist (first letter, first letter, tenth letter, etc.)
5. VIC Cipher
   1. Each of the preceeding challenges should give clues that they're dealing with a VIC cipher. (Even googling nickel year cipher should lead them in the right direction)
   2. Decoding the cipher leaves a set of coordinates
   3. looking at those coordinates on google maps spells out the flag