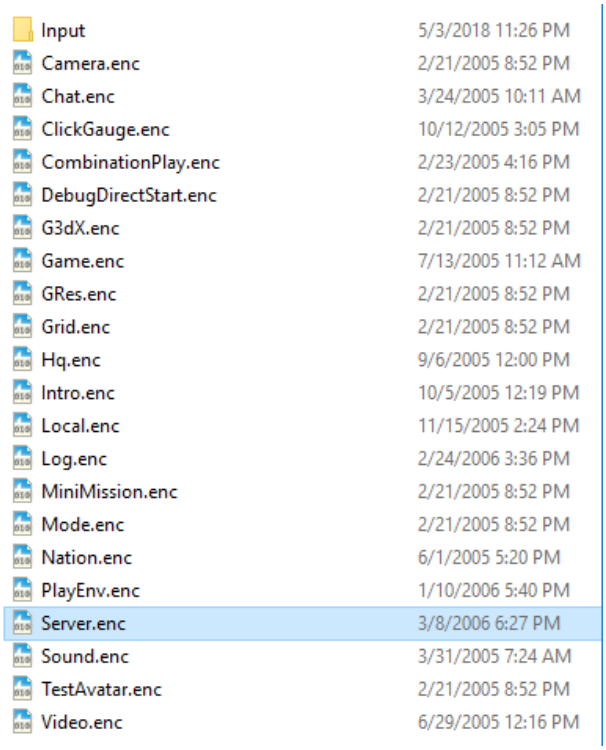
Daniel Hoynoski

Golf King Client Version: v0.34f

Turn In (extended): Friday, May 4th, 2018

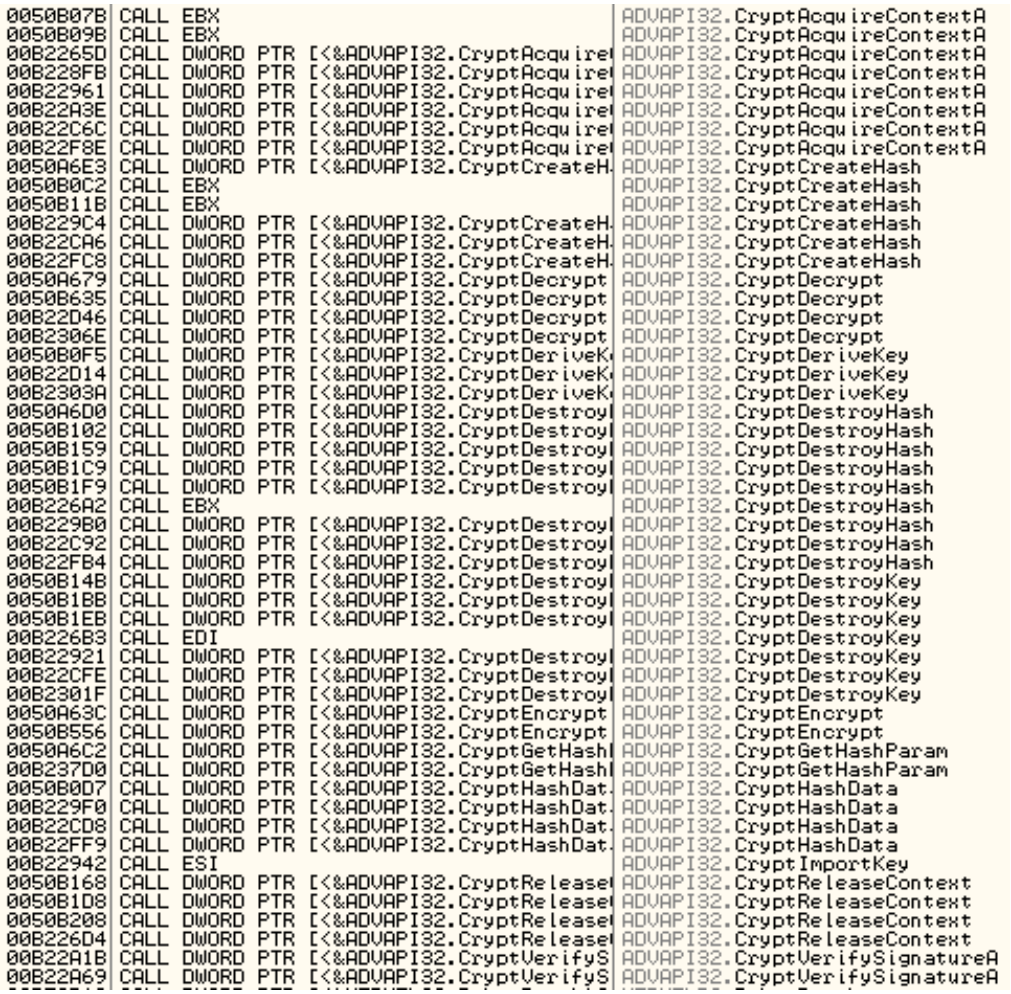
Game Crack 3 - The Encryption Wall Falls!

For the last big progress I made during the semester on getting some game-play back, I turned my attention to figuring out what was in all the encrypted files. Take for example these files:



Files such as “server.enc” and “local.enc” looked very promising for offering some more options and information on this game and how it worked. However, these files are hopelessly encrypted with RSA based encryption (discussed below).

Obviously the game has to decrypt the files at some point of execution, so I figured I would analyze the binary to see if I could find any useful information:



While looking at the intermodular calls the game was making, I noticed some very useful calls! In particular, I noticed two: CryptDecrypt and CryptEncrypt. My thoughts at this moment figured the game could also re-encrypt the files too (which would be a plus for testing).

These cryptographic functions are part of Microsoft's CryptoAPI, a very well documented and easily assessable API! My next task was to create a C program that reproduced the steps that the game did in its binaries. It was NOT easy and after LITERAL days of reversing and researching the cryptoAPI, I produced 414 lines of code that mimicked this encryption/decryption process (see crypto.c). Because you cannot just use decrypt/encrypt functionalities right away, an environment has to be setup correctly.

I set breakpoints at all the CryptoAPI function calls and then ran the game. I noticed the order in which the functions were being called in (i.e. for setting up the environment) and the parameters it was using. I even got the secret encryption key it was holding out on me:

0xEA, 0xCA, 0x31, 0x01

I was quite surprised to find that this key could be used to re-encrypt the files and after looking at the encrypted files in the game, the local.enc file allowed me to setup a local game (i.e. against the computer). The file was obviously kept for internal debugging for the programmers.

And to my dismay, I finally got game play:

In the above screenshot, I am using the English client I got my hands on, but the same code works for the Korean client too.

To view:

Please go to https://github.com/uiucseclab/hoynoski/blob/master/Game%20Cracking/Crack%203/crypto.c in order to view the encryption algorithm code I created.