WCTF CyKorPath Write-Up

The virtual machine uses a total of 6 registers. There are a total of 4 general purpose registers, a stack pointer, and a program counter.

The analysis of the processer of the virtual machine's instruction is shown at “processor.c”Í

Use a stack and use two additional independent memory spaces.,

Logic itself does not have any tricks, and the instruction is intuitive, so analysis is not difficult.

If you analyze all instruction, you can realize that program works like “problem.c”. So, I want to explain with “problem.c”.

Key file header is unique. Public key file signature is “K-PUB\x00”, Private key file signature is “K-PRIV”. And there is fixed base value, 128. If you are wrong with this, program will print “something wrong”.

Also, file has checksum by easy xor operation. Public key has already good checksum so you don’t have to fix it. When you make the private key file with private key, you should make checksum and checksum logic is easily to anlayze.

There is big number add operation. Add W[0] by key[0] times, and add W[1] by key[1], and so on…

Actually, this is multiplication. add all W[i]\*key[i] and compare with W[KEY\_LEN].

This is knapsack problem.

텍스트이(가) 표시된 사진

자동 생성된 설명

You can extract all public key(W[0],…W[63]), and ans(W[KEY\_LEN]). Knapsack Problem can be efficiently solved when density is low.

텍스트이(가) 표시된 사진

자동 생성된 설명

So you can get private key with LO algorithm. This solution is in “solve.sage”.

Now, you get the private key and then make private key file. This solution is in “make\_priv.py”

“CyKorPath.exe key.pub key.priv” : You can get the FLAG!