

Decrypting the key

```
1 $cert = New-Object -TypeName System.Security.Cryptography.X509Certificates.X509Certificate2
2 $cert.Import($pub_bytes)
3 $encKey = $cert.PublicKey.Key.Encrypt($key_bytes, $true)
4
```

This is the code we will use to decrypt the key.

If we print the key after the decryption script runs, we have something that looks reasonable.

It would be good to save the values to files.

```
\malware> $key_hex | Out-File key_hex.txt
\malware> $Key_Bytes | Out-File key_bytes.bin
```

Decrypting Alabaster's Password Database

The malware uses function Enc_Dec-File to encrypt and decrypt files using AES encryption. The other function, enc_dec, just keeps 12 jobs running at a time, and each of those jobs are just calls to Enc_Dec-File. We only have one file to decrypt, so we can skip enc_dec. Note: remember that Enc_Dec-File wants the binary version of the key.

You should be able to use the malware function to decrypt Alabaster's file. The easiest way is to paste the code of the function into a new tab (remove the function line and the closing brace.) Then write lines above the ex-function to give it the values it needs for \$key (binary version of the key), \$file (path to Alabaster's wannacookie file), and false (you do want to decrypt, I assume.)

Once you decrypted Alabaster's file, you will find it is a sqlite3 database. You can learn to read the database using information [here](#). Installation shouldn't be necessary if you use sqlite3 in a Linux VM. Find the name of the database, then the name of the table. Once you know that you can use a SELECT statement to dump the table. Or, you can just see if the file contains any text...

Hand in

- 1) What is Alabaster's password for the vault?