**Week 2 Work Shop**

**Flag: THM{SQL\_INJECTION\_MASTER}**

**Task: 2**

**Message: Hello!**

**256 Bit Encryption Key** 47C79F15C6EB01B6E90F031D4736851B

**Encrypted text:** WF3EtEDnkIdKLsc0O0r1Ug==

**Task 3.1**

**Public key**

MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCXQSXZGQ39X6VEsCXEl6M1rYPymzGZ3HvR9ziD5RBl5nqR13ppIdtrKqCAivmgCxkB76B814AsJ8WgMruWF+HqDiaM1tysog6/LuCVCAbogQSo/HwbHWRT0b9aWgQljv3r03uXOmTGfbQG8NVx97OL4ZMIqfUj59/ebHOjuq9PvQIDAQAB

**Private Key**



**Task 3.2 and 3.3**

Message:

‘Hello message’

Encrypted text: Zfofs8Y1Kq6ZiWpn8aavR3gbdT9v4EeZTGOpFYMiUWlPZ5s6zlLixoAsqTgYzzJnTnfBDUNxwcHy2Dl7BpGVDPASX0pFZlvA6iJWZPAXS0UeTTbQleJPf42jbOODA0fzgInfqkzWC3s0s3kWjnxWi1QisH5hnuzQYDp2SDl9aZs=

This is very interesting, I am still wrapping my head around how the private key gets wrapped up into the public key or works to decrypt the message. I know it was discussed, I just don’t quite get it yet.

I have wondered how companies claim to have secure messaging that not even they can decrypt and this sheds light on that.