Assignment 10. Hashes, DHE …

Crypto basics 1

Im far too lazy to put anything meaningful here. Instead, here's some information about what you just solved.$HEX[0a]The MD5 algorithm is a widely used hash function producing a 128-bit hash value. Although MD5 was initially designed to be used as a cryptographic hash function, it has been found to suffer from extensive vulnerabilities. It can still be used as a checksum to verify data integrity, but only against unintentional corruption.$HEX[0a]Like most hash functions, MD5 is neither encryption nor encoding. It can be cracked by brute-force attack and suffers from extensive vulnerabilities as detailed in the security section below.$HEX[0a]MD5 was designed by Ronald Rivest in 1991 to replace an earlier hash function MD4.[3] The source code in RFC 1321 contains a "by attribution" RSA license. The abbreviation "MD" stands for "Message Digest."$HEX[0a]The security of the MD5 has been severely compromised, with its weaknesses having been exploited in the field, most infamously by the Flame malware in 2012. The CMU Software Engineering Institute considers MD5 essentially "cryptographically broken and unsuitable for further use".[4]$HEX[0a]ctf{1_h0p3_y0u_d1dn7_d0_7h47_by_h4nd}$HEX[0a]

Done by this code.

Crypto basics 2

38058349620867258480

Done by this code.

Crypto basics 3

Found some base64 at the end of the file, decoded, got type of file via file command, got that that it is pgp message and key.
Bruteforced passphrase through:

```
JohnTheRipper/run/gpg2john key.xxx > hashes.xxx
JohnTheRipper/run/john hashes.xxx
```

Got pass: elviselvis

Decrypted via:

```
gpg --import key.xxx
gpg --decrypt xxx.1
```

Flag:

```
elvissiguevivo
```