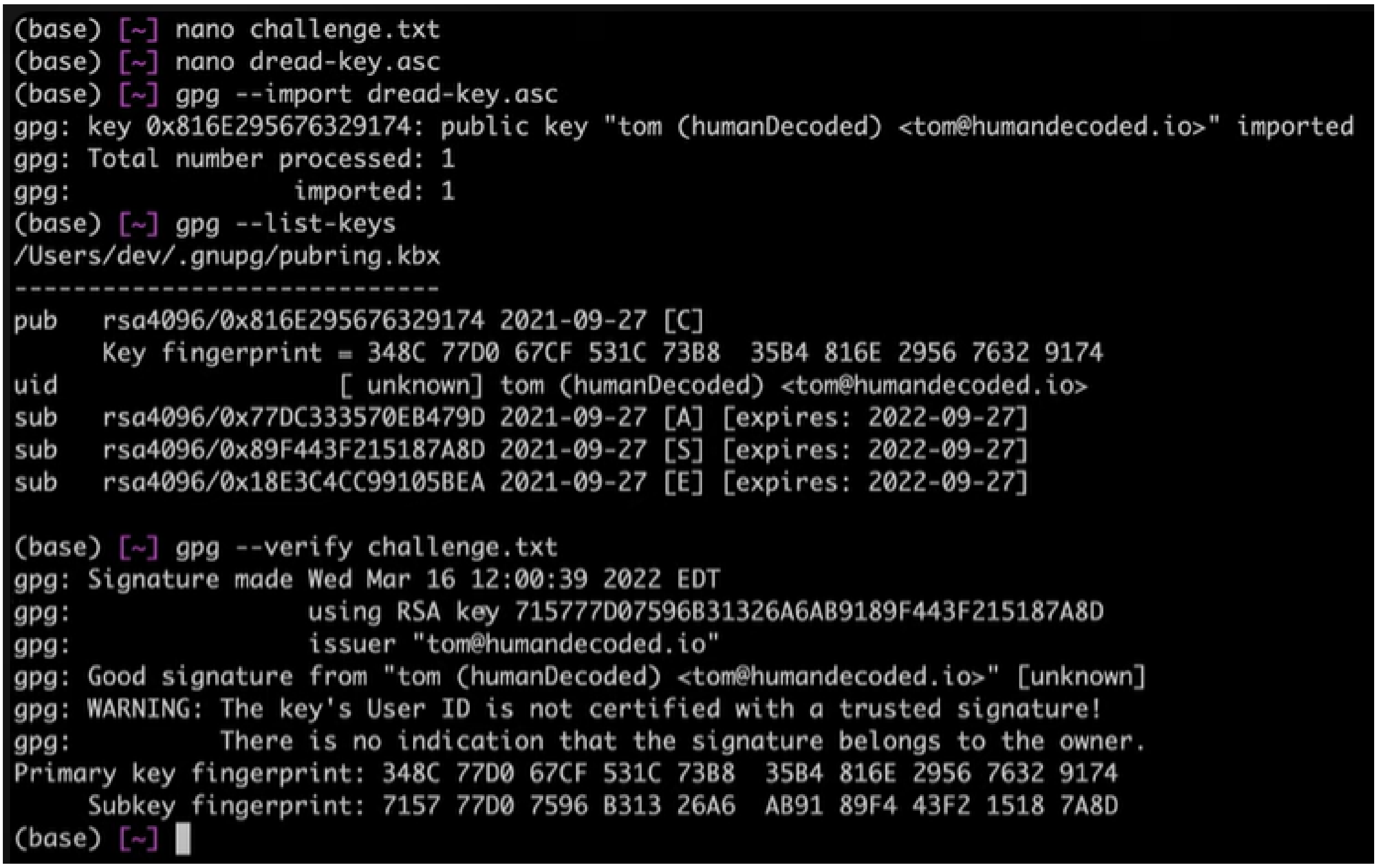
PGP/GPG

Make a *challenge.txt* file for the challenge.

Make a *publickey.asc* file for the Public PGP key.

The public key can be safely uploaded to your keyring:

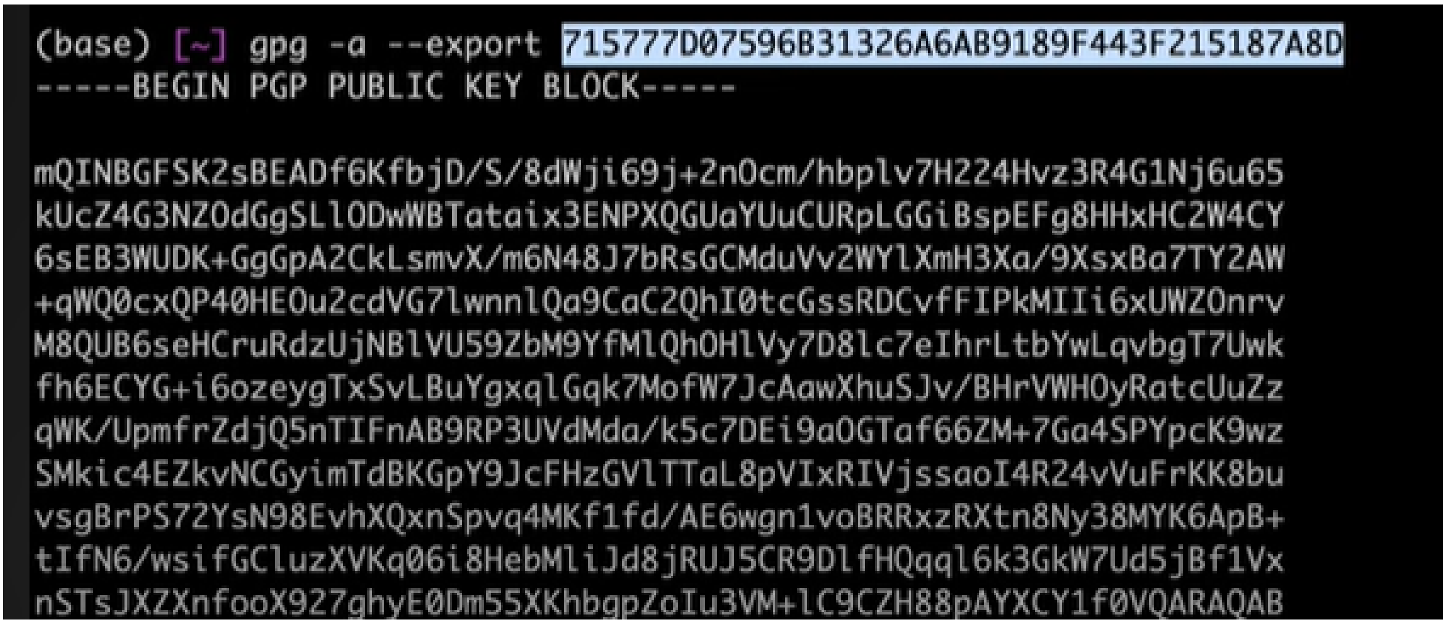
> *gpg --import publickey.asc*
>
> > info displayed is easily spoofed.
>
> *gpg --list-keys*
>
> > *List will show pub and sub keys. Subs are for [S] signing, [E] encryption, and [A] for authentication.*
>
> *gpg --verify challenge.txt*



```
(base) [~] nano challenge.txt
(base) [~] nano dread-key.asc
(base) [~] gpg --import dread-key.asc
gpg: key 0x816E295676329174: public key "tom (humanDecoded) <tom@humandecoded.io>" imported
gpg: Total number processed: 1
gpg:               imported: 1
(base) [~] gpg --list-keys
/Users/dev/.gnupg/pubring.kbx
-----------------------------
pub   rsa4096/0x816E295676329174 2021-09-27 [C]
      Key fingerprint = 348C 77D0 67CF 531C 73B8  35B4 816E 2956 7632 9174
uid                   [ unknown] tom (humanDecoded) <tom@humandecoded.io>
sub   rsa4096/0x77DC333570EB479D 2021-09-27 [A] [expires: 2022-09-27]
sub   rsa4096/0x89F443F215187A8D 2021-09-27 [S] [expires: 2022-09-27]
sub   rsa4096/0x18E3C4CC99105BEA 2021-09-27 [E] [expires: 2022-09-27]

(base) [~] gpg --verify challenge.txt
gpg: Signature made Wed Mar 16 12:00:39 2022 EDT
gpg:                using RSA key 715777D07596B31326A6AB9189F443F215187A8D
gpg:                issuer "tom@humandecoded.io"
gpg: Good signature from "tom (humanDecoded) <tom@humandecoded.io>" [unknown]
gpg: WARNING: The key's User ID is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: 348C 77D0 67CF 531C 73B8  35B4 816E 2956 7632 9174
     Subkey fingerprint: 7157 77D0 7596 B313 26A6  AB91 89F4 43F2 1518 7A8D
(base) [~] 
```

> *gpg -a --export 71577D0.....* the -a is ASCII Armor since PGP format is binary.



```
(base) [~] gpg -a --export 715777D07596B31326A6AB9189F443F215187A8D
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQINBGFSK2sBEADf6KfbjD/S/8dWji69j+2nOcm/hbplv7H224Hvz3R4G1Nj6u65
kUcZ4G3NZOdGgSLlODwWBTataix3ENPXQGUaYUuCURpLGGiBspEFg8HHxHC2W4CY
6sEB3WUDK+GgGpA2CkLsmvX/m6N48J7bRsGCMduVv2WYlXmH3Xa/9XsxBa7TY2AW
+qWQ0cxQP40HEOu2cdVG7lwnnlQa9CaC2QhI0tcGssRDCvfFIPkMIIi6xUWZOnrv
M8QUB6seHCruRdzUjNBlVU59ZbM9YfMlQhOHlVy7D8lc7eIhrLtbYwLqvbgT7Uwk
fh6ECYG+i6ozeygTxSvLBuYgxqlGqk7MofW7JcAawXhuSJv/BHrVWHOyRatcUuZz
qWK/UpmfrZdjQ5nTIFnAB9RP3UVdMda/k5c7DEi9aOGTaf66ZM+7Ga4SPYpcK9wz
SMkic4EZkvNCGyimTdBKGpY9JcFHzGVlTTaL8pVIxRIVjssaoI4R24vVuFrKK8bu
vsgBrPS72YsN98EvhXQxnSpvq4MKf1fd/AE6wgn1voBRRxzRXtn8Ny38MYK6ApB+
tIfN6/wsifGCluzXVKq06i8HebMliJd8jRUJ5CR9DlfHQqql6k3GkW7Ud5jBf1Vx
nSTsJXZXnfooX927ghyE0Dm55XKhbgpZoIu3VM+lC9CZH88pAYXCY1f0VQARAQAB
```

Match keys...

Credit: *humanDecoded at Trace Labs*