VE475
Introduction to Cryptography

Challenge 3

Manuel — UM-JI (Summer 2022)

- Break into a computer
- Forge a certificate
- Rewarded by a bonus on the final grade

The goal of this challenge is to complete at least one of the following two tasks:

- Somehow you learn that a server contains an ssh authorized_keys file wth the following line.

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAAUQDO2+ek1EGJdxXtecQwUsmVnA4oJPQ2qWq/VNcb0jn/KGF/
m3Q+m2UV/+VnJmT0qGSvnjyspERPc8wI0qC6Krz+oHfEBqb57w/FOfTbK02+VQ== attacker@weak
```

- Generate a fake certificate signed by the VE475 authority.

```
-----BEGIN CERTIFICATE-----
MIIDezCCAmOgAwIBAgIUHza8QhCJLIBMnWCu7KDeiLC0hOAwDQYJKoZIhvcNAQEE
BQAwTTELMAkGA1UEBhMCQ04xCzAJBgNVBAgMAkNBMRMwEQYDVQQKDApGT0NTLCBJ
bmMuMRwwGgYDVQQDDBNmb2NzLmppLnNqdHUuZWR1LmNuMB4XDTIyMDcyNjE0Mzcy
NVoXDTIzMDcyNjE0MzcyNVowTTELMAkGA1UEBhMCQ04xCzAJBgNVBAgMAkNBMRMw
EQYDVQQKDApGT0NTLCBJbmMuMRwwGgYDVQQDDBNmb2NzLmppLnNqdHUuZWR1LmNu
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtxAeDyQXYUhKe5Wxc17H
de6n63zY/hf0eMnO2eFCZ9xeTMY5hzMSNcUmY5KMnNZbDXSsu8mGdkivW77i+y2N
xN+n+EMNIVtcaa9Nru/K8iTOtNmpu+ihGWzjvQ8oTpqIRtkRTjx7BruWF34rNPJy
wAC2sGyRhIixFy2rTeGxcKFn/BmtpZXT4fKMMvL9H27qhF/3boz+AGm0vw8GnlN4
pVjCf/wVuRhr8IHpyAt2jjBsOFeFDnliSVO2Hgs3nXmH+B+wS4/7aJM62NNadO6I
iXe18bPnQf5r/HvtzoNaOH7XZ8KFA1UsR0VbkKuTfD9P2J3UpCJZHj8OOOH9jyBB
iwIDAQABo1MwUTAdBgNVHQ4EFgQUG7spjgOl1Fo80InaOLvJ9ZWTZ1QwHwYDVR0j
BBgwFoAUG7spjgOl1Fo80InaOLvJ9ZWTZ1QwDwYDVR0TAQH/BAUwAwEB/zANBgkq
hkiG9w0BAQQFAAOCAQEAXRmT8l2aDgqMgpd0iDvofIU2hrw0nkpa//taN+Ae6f18
o449P628HaGja7gVibHBpfh7H/ZSluHwvthplaTIdNRG8hH0HNfpdiWd1yNNQQsu
ZUJzHu9CEOs7myTjC280Wu66AxyIcHDPFVY0wc/fWc6nSlYJAyjKmdoGojdxNpFk
sGpxMIoYREUl9MtYOk/tG4Qrw9k892D19cfVrXco8LHc39fdweonSwk2kVApe2YC
1UrYDvv+Xbd+bxJgDnRofPMwRkU3uqLQmsGkoPNvNbF1kKAqIPcIOKMFuFNgrStQ
qAeq4j213udJS20fcAKFmwZN7T02fP9Hr8y/VNfLNg==
-----END CERTIFICATE-----
```

Rules and reward:

- No limitation on the number of students in a team
- Five points reward on the final grade per part of the challenge completed
- Only the first team to complete a part of the challenge will be rewarded
- The reward is to be shared among all the team members
- As soon as a part of the challenge is completed send us the corresponding proof by email
- The email submission deadline is August 6th, 23:59