VE475
Introduction to Cryptography

Challenge 3

Manuel — UM-JI (Summer 2021)

- 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 AAAAB3NzaC1yc2EAAAADAQABAAAAQQC8TpOkwL8MIlg225Rm7yTCHo7ronK3Ry0Yx/6c1wnq04o9
27bxUV/ZZDeCtRTVM4EDQrzdsLHK8Y0DGA1mt6yx attacker@weak
```

- Generate a fake certificate signed by the VE475 authority.

```
-----BEGIN CERTIFICATE-----
MIIDezCCAmOgAwIBAgIUHdF5ICArRiBkeoVoNQHmHwrFwcAwDQYJKoZIhvcNAQEE
BQAwTTELMAkGA1UEBhMCQ04xCzAJBgNVBAgMAkNBMRMwEQYDVQQKDApGT0NTLCBJ
bmMuMRwwGgYDVQQDDBNmb2NzLmppLnNqdHUuZWR1LmNuMB4XDTIxMDcxOTE2MjM1
MVoXDTIyMDcxOTE2MjM1MVowTTELMAkGA1UEBhMCQ04xCzAJBgNVBAgMAkNBMRMw
EQYDVQQKDApGT0NTLCBJbmMuMRwwGgYDVQQDDBNmb2NzLmppLnNqdHUuZWR1LmNu
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEArC/GIzM6rrn4iGida4dP
vHj6sx8V4wN8Je8SMoRLwmlpghRK/+2HdeMrjQGJDt7/bmFZslgiiW0ZQr84JfdF
hXquFKFVCt/eyU6pc/Tpw3YNTsql/SvskBRq2f8jUC8l+xHNoVWBavEgzAdxokKy
4WxES78pEAUiMIJRKzW3VLEM3Rt+jNcN2SnWYBP7XQXoT9ao6dueq3AGHg0zuH3B
nd5/UM911Yr+gv56Mil4BkGiTz78s8E3haVm5efTHxy1mWHq4sjV/3dhIpEGCJYc
X7i5CP5qGLsBbwqhv8ULrAtCYCSH5Zci67+Y8s5e5QijG/u/OGeeT4PNYW33BKDZ
OwIDAQABo1MwUTAdBgNVHQ4EFgQUKFkrZmumBoOiwadWVHzopC5nm3kwHwYDVR0j
BBgwFoAUKFkrZmumBoOiwadWVHzopC5nm3kwDwYDVR0TAQH/BAUwAwEB/zANBgkq
hkiG9w0BAQQFAAOCAQEAaFCwj0QniPmHF1xgO/BXtIKopiu5nmBdWdgX7yUrN+Oh
LU7MtCUAimEvhWi4muaw8XURzTotLD9z5OXFfYJQmYLqsnBO+BXD2BCOPHWNwVrD
LfDnb8cfki9DLnXmk3GmWpXpFyfwawCRCRo+QZTUicG17iHFsGzDE2Hh9eNSD57G
qdioBvwJ2wxUH8Zb+BU9dxLD5T0maaeFtUOx90C/vmGVo3dEl6zp8FQzy05owbY0
YBKTwtHtqE4XvCD63X11xqFoazttzbmbMLIQFFd5uKmpXpRXuacqNxhAaXbqt7mh
rd/ZZObBdJxNuVuo/cHNDvanP3DJH99gGPcABn1DlQ==
-----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 8th, 23:59