Denys Shabelnyk
ViA-KI-2022

Applied Cryptography

1. Generate a private key using OpenSSL: source: https://slproweb.com/products/Win32OpenSSL.html

`openssl genrsa -out acprivate.pem 2048`

```
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQC6k8eMsBXzAYkr
k7IdhvC6/xdM1jSAWDR5eHpW0NY/J/rlsjKiV3+piBzqJK3ePUFNql3oB5iqTm9w
Bsfnj3yt8xDB/qP4PPGBnAdb9cFGKJNuOBSdopIZtXiKJsMKn6OGt6Bos5HWeoA9
n3pi1HHdSeqZwcadcGBmouwSan5P/99E1kFgOZoD1jbyd432H1P9vAMjWgLPG6us
hG3PkDPzs5nHOrKhCJD9iuqw23bw2EsA/jpE8AAS1eflJ7TO3otwonPneCl4YhJs
k1nnWXEcV310dXp0A/XcwgTc6MylukWRkM8TyTQQc3hoHR4bAhyf6lLQ9BD/7jdT
m6AL9vvdAgMBAAECggEAJYcf9h5c69n9OzSj+Ohxd0tj5mKXgNE9DMm84cVzspRa
FOV45cpvtSvZlQb3qeHsRrDj3o3YmTjZlVDn2J212E8xqbOMS5wGf6lgmZCe5Xu3
282P5/0RIfasXi1ZwcNGYwyASU8FIHzXWo2/Ui2lEXuSooalanl2Cm7uyO1+ppxa
w9nmYQKA+YT2FoF0uNC0UqzaReSspVToW6cnPB0jeVE/39K9MvRPVjnh/H/kgEgb
wx3dKwqXH5Fw//mFvtwQXBnSylPN3k2dA+r0fEui239LhPQ5RnA5XDsTuQkN+Ucl
pNfYZg4wmSn5z6ShbsX0lflOwvMIG6ea51Gx9w+xiQKBgQDPVXrnhwW8iCucvVJH
u+R40oLQwaWL9KtVa2P92KcFj45YAbJ6SZiuH8+QsrQ3gl0n4x/biShKebDdGF66
cgau2HqH3ixoxuiz9O1i3Z9Pmbg+GZBZ94PbdPatMC93H0hsYTMuu5JJSsf6SQVk
FaxcCAM9ulQgJEXPDVdMeU9bwwKBgQDmXwzZYlUc/MZNs5TXGTnw0LOQ3fA62BQE
rYCNG/8iYWmh67NkKPRACPAh0k3p8IIgr0vHeD2Wj7IF/rloggSBRr3yZz2IfQyM
2joYnG00IcACaLBCk2Mrrkgth7t9VKEFqXFLZs6n0rWShTJZvvedU8ckE3GfPXbz
u+d4znnv3wKBgAvlK5f89ydJ6LalZgMXlJQZ/8daVNUixHGyJ5p4w5xeEBycfFDn
yAq1aIM0vYIxyIZxUXKW++jJ8ou8yjKIODnv0ZfZ91JLly477yKs9GbsutVVQiLn
QHlmzIBDM3XyJYWSTg1wVYQ+9ho19kk3tRvSmd0Aw7LUYezvJwMMMrFhAoGBAJDz
NY6CRLOciNnTKM++26oeZx27x6/+zXm0AbLH7tyfFmv/djyLWEQCW7WsMcIExpvy
MGgty/K0L3t+LwMG6/a7oECpnRoINKFbnjpmEoA+zCW34U/ClR+i5V9gjCPr3/VE
DDk5UsZd2kl67ZdyhTLEyAR3B4L+lZ3+mUJ2CFtZAoGAbRaTPlbxIN5e80PDXy7s
1POIyYyCGxQsPg8OzJGRBBwvFf6ts8zkv4faeRTVMIWhSXU51gB+gC3o4xRl+9/x
MPdHLvRGFr6+TihJquXcbNdK97NXLt99lU49LSp84FUgMwUYjlx/H/M2vfOEHaRn
BpjovpQlaoQBjgMth3UckV8=
-----END PRIVATE KEY-----
```

2. Generate a public key to private using OpenSSL:

```
openssl rsa -in acprivate.pem -pubout -out acpublic.pem
```

```
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAupPHjLAV8wGJK5OyHYbw
uv8XTNY0gFg0eXh6VtDWPyf65bIyold/qYgc6iSt3j1BTapd6AeYqk5vcAbH5498
rfMQwf6j+DzxgZwHW/XBRiiTbjgUnaKSGbV4iibDCp+jhregaLOR1nqAPZ96YtRx
3UnqmcHGnXBgZqLsEmp+T//fRNZBYDmaA9Y28neN9h9T/bwDI1oCzxurrIRtz5Az
87OZxzqyoQiQ/YrqsNt28NhLAP46RPAAEtXn5Se0zt6LcKJz53gpeGISbJNZ51lx
HFd9dHV6dAP13MIE3OjMpbpFkZDPE8k0EHN4aB0eGwIcn+pS0PQQ/+43U5ugC/b7
3QIDAQAB
-----END PUBLIC KEY-----
```

3. Decrypte private key and watch ASN.1 code source: https://holtstrom.com/michael/tools/asn1decoder.php

Input

```
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQC6k8eMsBXzAYkr
k7IdhvC6/xdM1jSAWDR5eHpW0NY/J/rlsjKiV3+piBzqJK3ePUFNql3oB5iqTm9w
Bsfnj3yt8xDB/qP4PPGBnAdb9cFGKJNuOBSdopIZtXiKJsMKn6OGt6Bos5HWeoA9
n3pi1HHdSeqZwcadcGBmouwSan5P/99E1kFgOZoD1jbyd432H1P9vAMjWgLPG6us
hG3PkDPzs5nHOrKhCJD9iuqw23bw2EsA/jpE8AAS1eflJ7TO3otwonPneCl4YhJs
k1nnWXEcV310dXp0A/XcwgTc6MylukWRkM8TyTQQc3hoHR4bAhyf6lLQ9BD/7jdT
```

Convert BASE64/PEM to ASN.1

Output

```
SEQUENCE {
   INTEGER 0x00 (0 decimal)
   SEQUENCE {
      OBJECTIDENTIFIER 1.2.840.113549.1.1.1 (rsaEncryption)
      NULL
   }
   OCTETSTRING
308204a30201000282010100ba93c78cb015f301892b93b21d86f0baff174cd63480583479787a56d0d63f27fae5b232a2577fa9881cea24adde3d414daa5d
e80798aa4e6f7006c7e78f7cadf310c1fea3f83cf1819c075bf5c14628936e38149da29219b5788a26c30a9fa386b7a068b391d67a803d9f7a62d471dd49ea
99c1c69d706066a2ec126a7e4fffdf44d64160399a03d636f2778df61f53fdbc03235a02cf1babac846dcf9033f3b399c73ab2a10890fd8aeab0db76f0d84b
00fe3a44f00012d5e7e527b4cede8b70a273e778297862126c9359e759711c577d74757a7403f5dcc204dce8cca5ba459190cf13c934107378681d1e1b021c
9fea52d0f410ffee37539ba00bf6fbdd02030100010282010025871ff61e5cebd9fd3b34a3f8e871774b63e6629780d13d0cc9bce1c573b2945a14e578e5ca
6fb52bd99506f7a9e1ec46b0e3de8dd89938d99550e7d89db5d84f31a9b38c4b9c067fa96099909ee57bb7dbcd8fe7fd1121f6ac5e2d59c1c346630c80494f
05207cd75a8dbf522da5117b92a286a56a79760a6eeec8ed7ea69c5ac3d9e6610280f984f6168174b8d0b452acda45e4aca554e85ba7273c1d2379513fdfd2
bd32f44f5639e1fc7fe480481bc31ddd2b0a971f9170fff985bedc105c19d2ca53cdde4d9d03eaf47c4ba2db7f4b84f4394670395c3b13b9090df94725a4d7
d8660e309929f9cfa4a16ec5f495f94ec2f3081ba79ae751b1f70fb18902818100cf557ae78705bc882b9cbd5247bbe478d282d0c1a58bf4ab556b63fdd8a7
058f8e5801b27a4998ae1fcf90b2b437825d27e31fdb89284a79b0dd185eba7206aed87a87de2c68c6e8b3f4ed62dd9f4f99b83e199059f783db74f6ad302f
771f486c61332ebb92494ac7fa49056415ac5c08033dba54202445cf0d574c794f5bc302818100e65f0cd962551cfcc64db394d71939f0d0b390ddf03ad814
04ad808d1bff226169a1ebb36428f44008f021d24de9f08220af4bc7783d968fb205feb96882048146bdf2673d887d0c8cda3a189c6d3421c00268b0429363
2bae482d87bb7d54a105a9714b66cea7d2b592853259bef79d53c72413719f3d76f3bbe778ce79efdf0281800be52b97fcf72749e8b6a5660317949419ffc7
5a54d522c471b2279a78c39c5e101c9c7c50e7c80ab5688334bd8231c88671517296fbe8c9f28bbcca32883839efd197d9f7524b972e3bef22acf466ecbad5
554222e7407966cc80433375f22585924e0d7055843ef61a35f64937b51bd299dd00c3b2d461ecef27030c32b1610281810090f3358e8244b39c88d9d328cf
bedbaa1e671dbbc7affecd79b401b2c7eedc9f166bff763c8b5844025bb5ac31c204c69bf230682dcbf2b42f7b7e2f0306ebf6bba040a99d1a0834a15b9e3a
6612803ecc25b7e14fc2951fa2e55f608c23ebdff5440c393952c65dda497aed97728532c4c804770782fe959dfe994276085b590281806d16933e56f120de
5ef343c35f2eecd4f388c98c821b142c3e0f0ecc9191041c2f15feadb3cce4bf87da7914d53085a1497539d6007e802de8e31465fbdff130f7472ef44616be
be4e2849aae5dc6cd74af7b3572edf7d954e3d2d2a7ce055203305188e5c7f1ff336bdf3841da4670698e8be94256a84018e032d87751e915f
}
```

4. Decrypte public key and watch ASN.1 code
source: https://holtstrom.com/michael/tools/asn1decoder.php

Input

```
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAupPHjLAV8wGJK5OyHYbw
uv8XTNY0gFg0eXh6VtDWPyf65bIyold/qYgc6iSt3j1BTapd6AeYqk5vcAbH5498
rfMQwf6j+DzxgZwHW/XBRiiTbjgUnaKSGbV4iibDCp+jhregaLORlnqAPZ96YtRx
3UnqmcHGnXBgZqLsEmp+T//fRNZBYDmaA9Y28neN9h9T/bwDI1oCzxurrIRtz5Az
87OZxzqyoQiQ/YrqsNt28NhLAP46RPAAEtXn5Se0zt6LcKJz53gpeGISbJNZ51lx
HFd9dHV6dAP13MIE3OjMpbpFkZDPE8k0EHN4aB0eGwIcn+pS0PQQ/+43U5ugC/b7
```

Convert BASE64/PEM to ASN.1

Output

```
SEQUENCE {
   SEQUENCE {
      OBJECTIDENTIFIER 1.2.840.113549.1.1.1 (rsaEncryption)
      NULL
   }
   BITSTRING
0x3082010a0282010100ba93c78cb015f301892b93b21d86f0baff174cd63480583479787a56d0d63f27fae5b232a2577fa9881cea24adde3d414daa5de807
98aa4e6f7006c7e78f7cadf310c1fea3f83cf1819c075bf5c14628936e38149da29219b5788a26c30a9fa386b7a068b391d67a803d9f7a62d471dd49ea99c1
c69d706066a2ec126a7e4fffdf44d64160399a03d636f2778df61f53fdbc03235a02cf1babac846dcf9033f3b399c73ab2a10890fd8aeab0db76f0d84b00fe
3a44f00012d5e7e527b4cede8b70a273e778297862126c9359e759711c577d74757a7403f5dcc204dce8cca5ba459190cf13c934107378681d1e1b021c9fea
52d0f410ffee37539ba00bf6fbdd0203010001 : 0 unused bit(s)
}
```