Main Tests

April 20, 2020

1 Main function tests, done by Charlie Cook, April 20th, 2020

[1]:
```
import pisgmMain
```

1.1 Create a random key to test with

[2]:
```
k = pisgmMain.rsa.keyObj()
```

1.2 Separate the public and private keys

[3]:
```
u = pisgmMain.rsa.publicKey(k.exportU())
```

[4]:
```
r = pisgmMain.rsa.privateKey(k.exportR())
```

1.3 Write a message

[5]:
```
message = "I've seen things you people wouldn't believe.\nAttack ships on fire␣
↪off the Shoulder of Orion.\nI watched C-Beams, glitter in the dark off a␣
↪Tannhauser gate.\nAll those, moments, will be lost, in time... like tears,␣
↪in rain.\nTime, to die."
```

1.4 Test the makeRequest function

1.4.1 (for testing, a uid of 13 is provided)

[6]:
```
reply = pisgmMain.makeRequest(r, u, 13)
```

```
Timestamp:  4 b'^\x9d\xdf\x80'
Nonce:  16 b'\x8d\xc4\x1b\xfd\x9b\xd8\xc2m\xf4S\x85p\x1e\xc8\x94\x9d'
Request:  24 b'^\x9d\xdf\x80\x8d\xc4\x1b\xfd\x9b\xd8\xc2m\xf4S\x85p\x1e\xc8\x94\
x9d\x00\x00\x00\r'
Signature:  256 b" \xb9\xa1v\x84M\x1c\xe95P|\xf2\x84D \x19\x0e\x8b9\xc1\xb7\xe0\
xae\xees\xd2\xa5j\x14\x90:\xc1\x9f\xd8\x1e[\xae\xa8\x8c\xc6\x0b\xf1\xa3m\n\x1aj\
xf1\xfe\xa8\xdc\x04M\xaa0&BD\x860\xc9B\xaf/\x96\x0b@\xf3\xeb\x82p\xe9\xd5\x14\xa
e^\xfb\xe6Z\x92\x8b\x1fW69\xb4\x98~\xfd\xa4\x97E$T\x89?k\xa6\xe2\xc95\xd28%\xfa\
t\x81\xc0\xb3\xe1\x91\n\x12\x90\xb5\xfb\xd9.\xd0\x9b$wvT}\xd1Y\xe8c\x83\x02$\xe3
```

```
\x9ash\xf6J\x84\xc1&7\xab\x1f\x15\xae\xdb!\xdb*\xc9\xeb\x18\x9a\x8cQ\xff\xfb\xe5
P\xc0B9d7\xf8l-K5\x91WG\xc9\x87\xe03x\xdf\xafQ\xbaH\x94\xf0\xa5\xa0\x0b$\x10\xe9
S\xbe@\xc0s\xeaW\x8c\x00Y\xfah\x01m)U\xd1\x00:\x1e\xebb\xb4_Wp\x91\xe7\x8f@\x96\
xa6e\x9a\x8c\x9eY\xa2\x19\xc9\x0bL\x8dN\x99\xbe\x8e\x00\xfe\xc8\x0f\x89M\xa5\xc8
m\x12\x9a('\x1c\t\xbe\xbbb"
```

1.5 Test the makeImage function

1.5.1 (in the reply tuple, 0 is the signature of the request, 1 is the nonce, and 2 is the requisitioned AES key)

[7]:
```
image = pisgmMain.makeImage(message, reply[0], reply[1], reply[2])
```

492

[8]:
```
image
```

[8]:

1.6 Convert the image back to raw data

[9]:
```
raw = pisgmMain.img.grayImageToBytes(image)
```

[10]:
```
raw
```

[10]:
```
b" \xb9\xa1v\x84M\x1c\xe95P|\xf2\x84D \x19\x0e\x8b9\xc1\xb7\xe0\xae\xees\xd2\xa5
j\x14\x90:\xc1\x9f\xd8\x1e[\xae\xa8\x8c\xc6\x0b\xf1\xa3m\n\x1aj\xf1\xfe\xa8\xdc\
x04M\xaa0&BD\x860\xc9B\xaf/\x96\x0b@\xf3\xeb\x82p\xe9\xd5\x14\xae^\xfb\xe6Z\x92\
x8b\x1fW69\xb4\x98~\xfd\xa4\x97E$T\x89?k\xa6\xe2\xc95\xd28%\xfa\t\x81\xc0\xb3\xe
1\x91\n\x12\x90\xb5\xfb\xd9.\xd0\x9b$wvT}\xd1Y\xe8c\x83\x02$\xe3\x9ash\xf6J\x84\
xc1&7\xab\x1f\x15\xae\xdb!\xdb*\xc9\xeb\x18\x9a\x8cQ\xff\xfb\xe5P\xc0B9d7\xf8l-K
5\x91WG\xc9\x87\xe03x\xdf\xafQ\xbaH\x94\xf0\xa5\xa0\x0b$\x10\xe9S\xbe@\xc0s\xeaW
\x8c\x00Y\xfah\x01m)U\xd1\x00:\x1e\xebb\xb4_Wp\x91\xe7\x8f@\x96\xa6e\x9a\x8c\x9e
Y\xa2\x19\xc9\x0bL\x8dN\x99\xbe\x8e\x00\xfe\xc8\x0f\x89M\xa5\xc8m\x12\x9a('\x1c\
t\xbe\xbbb\xc4\xf4jo`\x0b\x01k\xf8`\x92Dg\x81\x90\xde\x11~\xcc\x8fdm\xef\x98\x95
\x1cMZ\xe14\x18>\xc2\xab\xaa,\xf2D[<\xc1\xf0\x1er\xea\xe5\xc1\x9672y\x9b\xec!du'
\xcb\xb8\xb30\xd14\xf9&\xad\x10\xbe\xbc\x9c\x16\x8e\x90\xba\xc0\x05r\xc8M<f\xfa\
x06k \x9eF\xe8\xacyD\rX'\x05)\xd1\xe6j\xce\xce\xeb\xcb\x1d\x80\x956\x93au\xfc\xe
9\xde\nS\xab\x96\xf7\xd8\xfc\t\x99\xf6\xd2^\xf5l7wi@D\x0f6Xrj\xf1vv\xe0#i\xee\x8
4^${!)\xb6\xd6\xd5\xae\x05\xeaP\x87J\n\xaa/\xb9I`\xee(\xd7\x13w\xb4i\xe2\x80J\xa
c#\x94\xc9i!O\xf5d\x15ll\x01\x02S\x0c7\x17\x8d\x05\xcd>\xd2\xeam\x11\xfe\xb7&X\x
f5\xb4\x9c\xf7(\xd2\xb3\x1dT\xa2V\xa3\xfan\xb1\xf9\xe9!\x15\xfaF;\xd9\xcb\x89\xf
eM\xecQ\x02\x8e"
```

[11]:
```
len(raw)
```

[11]: 492

1.7 This byte matches the final byte of the signature, which is put at the beginning of the image. Thus, any bytes after it are ciphertext. To be safe, the length of the signature should be used in whatever `decryptImage` function is made

[12]:
```
hex(raw[255])
```

[12]: '0x62'

1.8 Extract the ciphertext

[13]:
```
c = raw[256:]
```

1.9 Make an AES Radio object for decryption

[14]:
```
radio = pisgmMain.aes.aesRadio(reply[2], reply[1])
```

1.10 Decrypt the ciphertext to see the original message

[15]:
```
m = radio.decrypt(c)
```

[16]:
```
print(m.decode("ascii"))
```

```
I've seen things you people wouldn't believe.
Attack ships on fire off the Shoulder of Orion.
I watched C-Beams, glitter in the dark off a Tannhauser gate.
All those, moments, will be lost, in time… like tears, in rain.
Time, to die.
```