

# step 1

a = [1,1,1,1,1,6]

b = [7,3,1,7,3,1]

c = 0

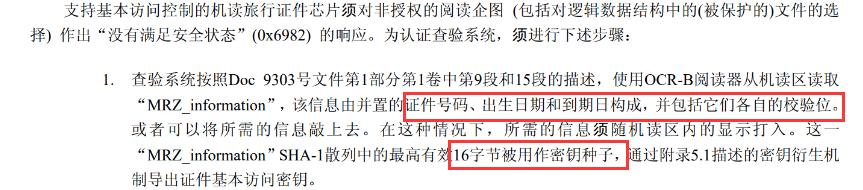
for i in range(len(a)):

c += a[i]\*b[i]

c %= 10

# print(c)

# 7



# step 2

passport = '12345678<8<<<1110182<1111167<<<<<<<<<<<<<<<4'

no = passport[:10]

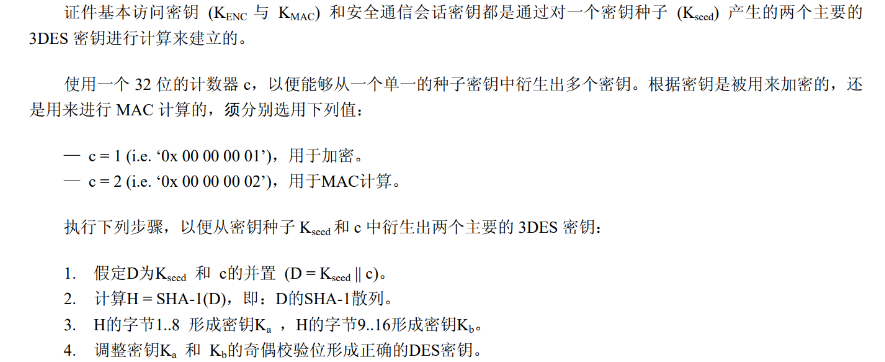
birth = passport[13:20]

arrive = passport[21:28]

mrz = no+birth+arrive

h\_mrz = sha1(mrz.encode()).hexdigest()

# print(h\_mrz)

# a095f0fdfe51e6ab3bf5c777302c473e7a59be65 

# step 3

k\_seed = h\_mrz[:32]

c = '00000001'

d = k\_seed + c

h\_d = sha1(bytes.fromhex(d)).hexdigest()

# print(h\_d)

# eb8645d97ff725a998952aa381c5307909962536

#step 4

ka = jiou(h\_d[:16])

kb = jiou(h\_d[16:32])

key = ka+kb

# step 5

cipher = '9MgYwmuPrjiecPMx61O6zIuy3MtIXQQ0E59T3xB6u0Gyf1gYs2i3K9Jxaa0zj4gTMazJuApwd6+jdyeI5iGHvhQyDHGVlAuYTgJrbFDrfB22Fpil2NfNnWFBTXyf7SDI'

cipher = base64.b64decode(cipher)

aes = AES.new(bytes.fromhex(key),AES.MODE\_CBC,bytes.fromhex('0'\*32))

result = aes.decrypt(cipher).decode()

print(result)

# Herzlichen Glueckwunsch. Sie haben die Nuss geknackt. Das Codewort lautet: Kryptographie!