```python
1   import hashlib
2   from Crypto.Cipher import AES
3   from Crypto.Util.number import long_to_bytes
4   import base64
5
6   mrz = "12345678<8<<<1110182<1111167<<<<<<<<<<<<<<<4"
7   # https://en.wikipedia.org/wiki/Machine-readable_passport
8   # passport number checksum 138%10 = 8, OK
9   pass_no = "12345678<"
10  check_digit1_9 = "8"
11  # birth no checksum 22%10 = 2, OK
12  birth = "111018"
13  check_digit14_19 = "2"
14  sex = "<" # unspecified
15  expiration_data = "111116"
16  # calc check digit on date domain
17  # date   : 1 1 1 1 1 6
18  # weight : 7 3 1 7 3 1
19  # mul    : 7+3+1+7+3+6 = 27 % 10 = 7
20  check_digit22_27 = "7" # unknown
21  check_digit_all = "4"
22
23  MRZ_inf = pass_no + check_digit1_9 + birth + check_digit14_19 +
    expiration_data + check_digit22_27
24  print("MRZ info: ", MRZ_inf)
25
26  key_seed = hashlib.sha1(MRZ_inf.encode()).hexdigest()[0:32]
27  d = key_seed + "00000001"
28  H_SHA1 = hashlib.sha1(long_to_bytes(int(d,16))).hexdigest()
29  ka = long_to_bytes(int(H_SHA1[0:32], 16))
30  Ka = ""
31
32  for i in range(16):
33      a = bin(ka[i])[2:]
34      while len(a) < 8:
35          a = '0' + a
36      if a[0:7].count("1") % 2 == 1:
37          Ka += a[0:7] + "0"
38      else:
39          Ka += a[0:7] + "1"
40
41  print("Secret Key:", hex(int(Ka, 2))[2:])
42  AES_key = long_to_bytes(int(Ka, 2))
43
44  iv = b"\0" * 16
45  cipher =
    base64.b64decode(b"9MgYwmuPrjiecPMx61O6zIuy3MtIXQQ0E59T3xB6u0Gyf1gYs2i3K9Jxaa
    0zj4gTMazJuApwd6+jdyeI5iGHvhQyDHGVlAuYTgJrbFDrfB22Fpil2NfNnWFBTXyf7SDI")
```

```python
aes = AES.new(AES_key, mode=AES.MODE_CBC, iv=iv)
message = aes.decrypt(cipher)
while message[-1] < 20:
    message = message[:-1]
print("message:", message.decode())
```