***Four-eye* principle**

To protect a secret code one uses a protection system that encrypts the code using the following *four-eye*-based protocol:

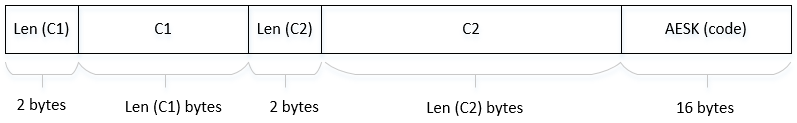
1. Random generate two initial secret keys ***k1*** and ***k2***, each of 64-bit length.
2. From ***k1*** and ***k2***, generates a secret key ***k*** using the computation ***k = SHA256 (k1 XOR k2)***
3. Encrypt the secret code with 256-bit variant of AES and using the secret key ***k***. The ECB mode and PKCS7 padding scheme are used for AES.
4. Encrypt each of the initial secret keys k1 and k2 using the RSA cryptosystem:

C1 = k1 ^ e1 mod n1,

C2 = k2 ^ e2 mod n2,

Where (e1, n1) and (e2, n2) are the RSA public keys of two key-officers, Alice and Bob.

1. Finally, all of these pieces are embedded in a single code-accessing blob using the next structure:



Whenever the secret code has to be accessed, the *4-eye* principle has to be applied meaning that both Alice and Bob use their RSA keys to get the secret needed to decrypt the code.

You have the mission to demonstrate this protection system is breakable and one could access the secret code with no requirement from the two key officers.

You can find bellow the code-accessing blob and the RSA public keys of the two key-officers.

Your flag is the secret code.

**The code-accessing blob** (hex encoding):

001893834DF42280C7A3D695ED87D986A2DD87E5BF43C4B5DEA50018172FFF3690221206BE2780BD99DC5A3C3A632D637595721D8E468C11326435BDA16CD0E7FDE4CC23

**Alice’s public key**:

-----BEGIN PUBLIC KEY-----

MIIBIDANBgkqhkiG9w0BAQEFAAOCAQ0AMIIBCAKCAQEAzjQuC7VtSzbFjU4FbEYx

MTWBQJTFh8zkXdiYhdDv/iH2k5XeZtm+6Zozz4MOrNRlyhcuqBjHyGmLp/DXz6VN

bHXQOSSFpnPXOM+W96xGFp/EJ4qhxLagcY7uFMfXS/tHIfKq1yxBPnmHnrDNGve2

taGhQaAyeXKkIn2X665aZgwzgVDiVjviBQFPqVT6U5HROOf6YzLhhPtCYaoiYLs/

gCLhJJfGu9POJuRVVPElEA0eQW7bxmXPSXQRRFbq4NIoFoYOV6YS+qzv1sbTn2Zh

I+pvT2HpdEvwx2S9L/j0PLdhCBQ7xUPX2Bg//d87JDYT1hOJImptwSVo0ZDaafvZ

7QIBAw==

-----END PUBLIC KEY-----

**Bob’s public key**:

-----BEGIN PUBLIC KEY-----

MIIBIDANBgkqhkiG9w0BAQEFAAOCAQ0AMIIBCAKCAQEAxXpbMNT1pMZaV/VwIDaO

sWW7XKY7bksSPpJ0NpleJl9wBmXEVh1HnWYFd9fdBtlsQXsVxqxUNBYS6FdsHzgp

G7Y0N7UZ4ISf3FKp12HmKxakfNM6Bj2rIYRPyFlCMZAvgmmKLNKgu8cm8cgKbSMe

msgdOoO46Ft11Ywa801sVCCEpXJFT7PVNepTYMhQ+vU8Mr8r/YPxwrKLxdoXh8XJ

tj7FrmylHCWYvA91QIQpe4h4i1XdlBcDg01rnNplJVJoDOI7agXCT9XsA8zNGJ++

iwoMT7Q+9xLOYVWw/rPjSBacpqH75DATpz7tMWw1bxPnXT1ShLTNnk41uB2qMZFf

ZQIBAw==

-----END PUBLIC KEY-----