[Lab7 CSLab task]

// Lab7 - no code work this week

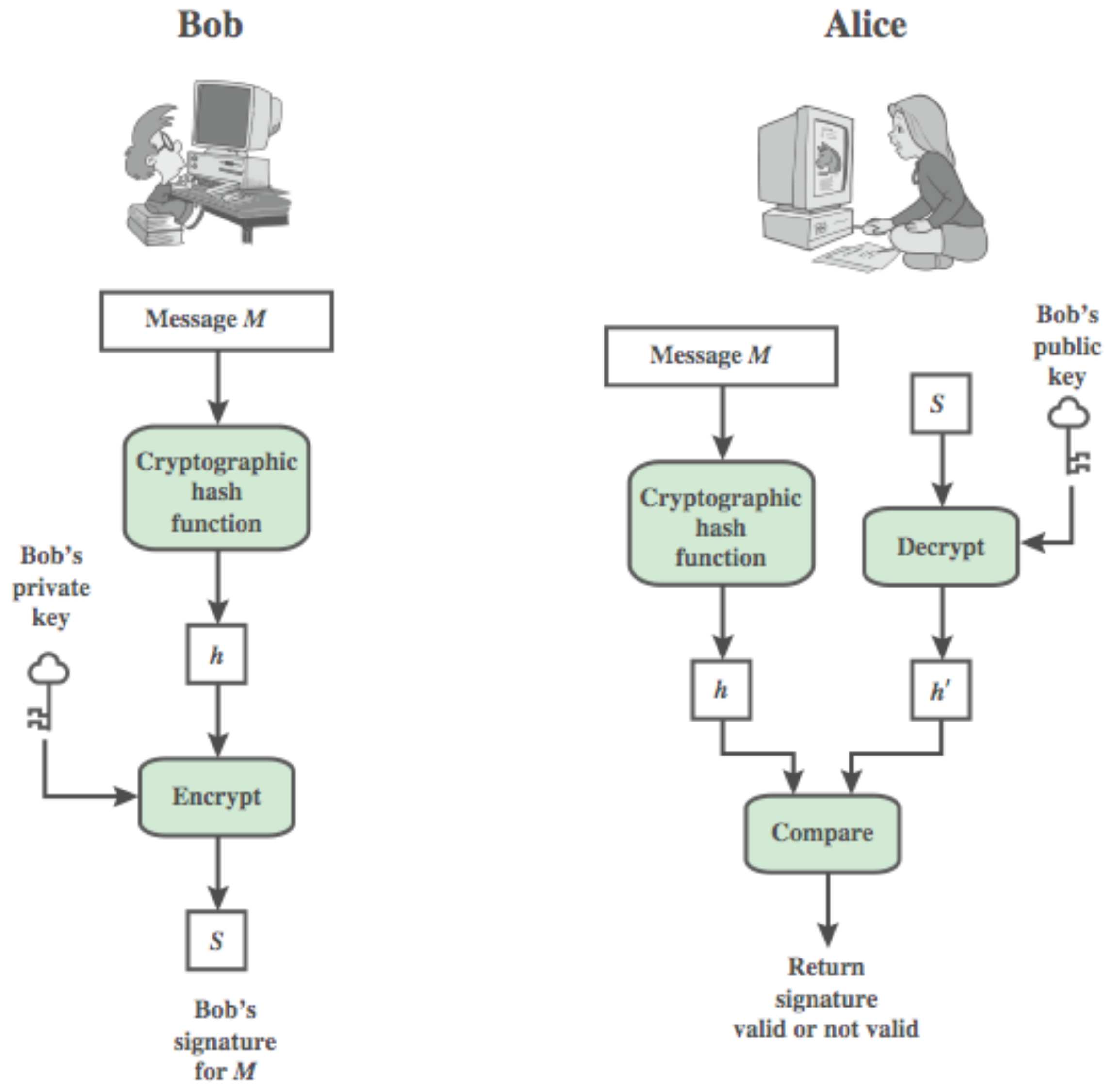
Online AES encryption and decryption:
http://rubbingalcoholic.github.io/cowcrypt/demos/aes.html

Online RSA encryption and decryption:
http://www-cs-students.stanford.edu/~tjw/jsbn/rsa2.html

Online digital signature algorithm:
https://kjur.github.io/jsrsasign/sample/sample-rsasign.html

Task 1. Demo of message authentication by digital signature

In this task, we use the *student ID* as the message M, and we employ SHA-256 as the cryptography hash function. The online digital signature tool is provided above.



Question table:

Message M:	s3613252

RSA private key:	-----BEGIN RSA PRIVATE KEY----- MIICWwIBAAKBgQDRhGF7X4A0ZVlE g594WmODVVUIiiPQs04aLmvfg8Sb orHss5gQ Xu0aIdUT6nb5rTh5hD2yfpF2WIW6M 8z0WxRhwicgXwi80H1aLPf6lEPPLvN 29EhQ NjBpkFkAJUbS8uuhJEeKw0cE49g80 eBBF4BCqSL6PFQbP9/ rByxdxEoAIQIDAQAB AoGAA9/q3Zk6ib2GFRpKDLO/ O2KMnAfR+b4XJ6zMGeoZ7Lbpi3M W0Nawk9ckVaX0 ZVGqxbSIX5Cvp/yjHHpww+QbUFrw/ gCjLiiYjM9E8C3uAF5AKJ0r4GBPl4u8 K4bp bXeSxSB60/ wPQFiQAJVcA5xhZVzqNuF3EjuKdHs w+dk+dPECQQDubX/lVGFgD/xY uchz56Yc7VHX+58BUkNSewSzwJRb cueqknXRWwj97SXqpnYfKqZq78dnE F10SWsr /NMKi+7XAkEA4PVqDv/ OZAbWr4syXZNv/ Mpl4r5suzYMMUD9U8B2JIRnrhmGZ PzL x23N9J4hEJ+Xh8tSKVc80jOkrvGlSv +BxwJAaTOtjA3YTV+gU7Hdza53sCn Sw/8F YLrgc6NOJtYhX9xqdevbyn1lkU0zPr8 mPYg/ F84m6MXixm2iuSz8HZoyzwJARi2p aYZ5/5B2lwroqnKdZBJMGKFpUDn7 Mb5hiSgocxnvMkv6NjT66Xsi3iYakJII 9q8C Ma1qZvT/ cigmdbAh7wJAQNXyoizuGEltiSaBXx4 H29EdXNYWDJ9SS5f070BRbAIl dqRh3rcNvpY6BKJqFapda1DjdcncZE CMizT/GMrc1w== -----END RSA PRIVATE KEY-----

Generated signature:	8428410924c524e618f2fe9363e58d2027c7b4af559772c5f5ed1a3b28fac378 ed1e86cbf26c05eedc5910d95c7446e7a3b01f6d51e9a9d7459e75a9c9b4adb6 a9210d50f29c4138c02b6591f42e3ca472d813b1b7d5eb61035df5cf866b94d4 627c8985613a7a375b37ca75f21339cf56af044a114056b46e31020a7e3f0efc

Task 2. Demo the process of getting student’s profile

In this task, we use the *student ID* as the student’s profile, and we employ AES (CBC mode) and 1024-bit key RSA to protect the data. Both online crypto tools are provided.

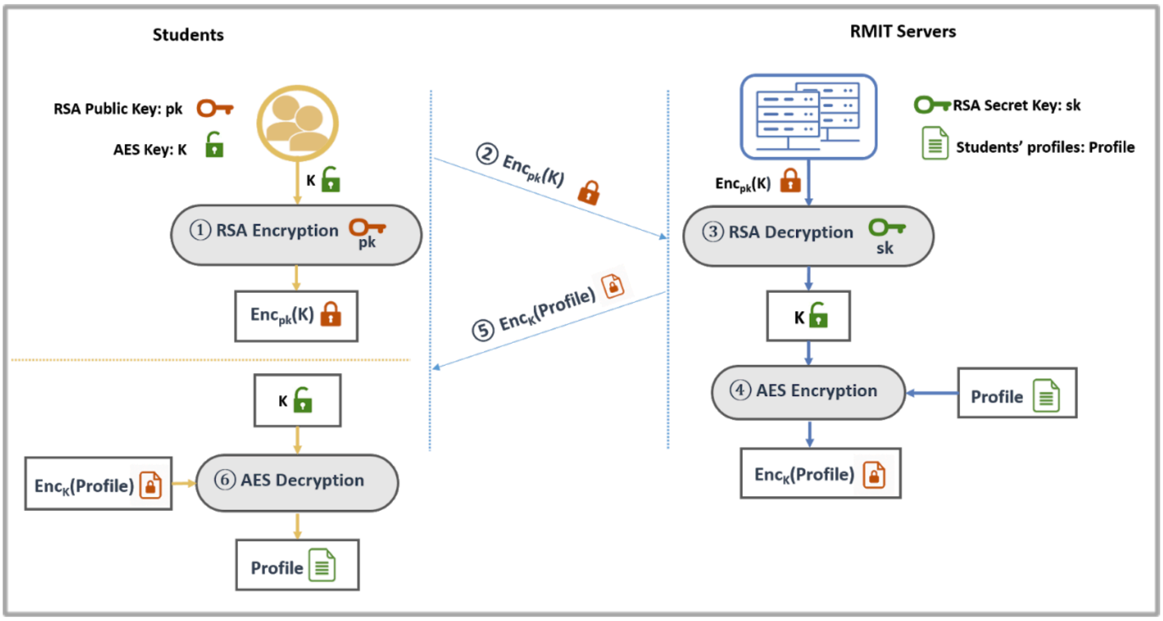


Figure 2. Process of getting student's profile

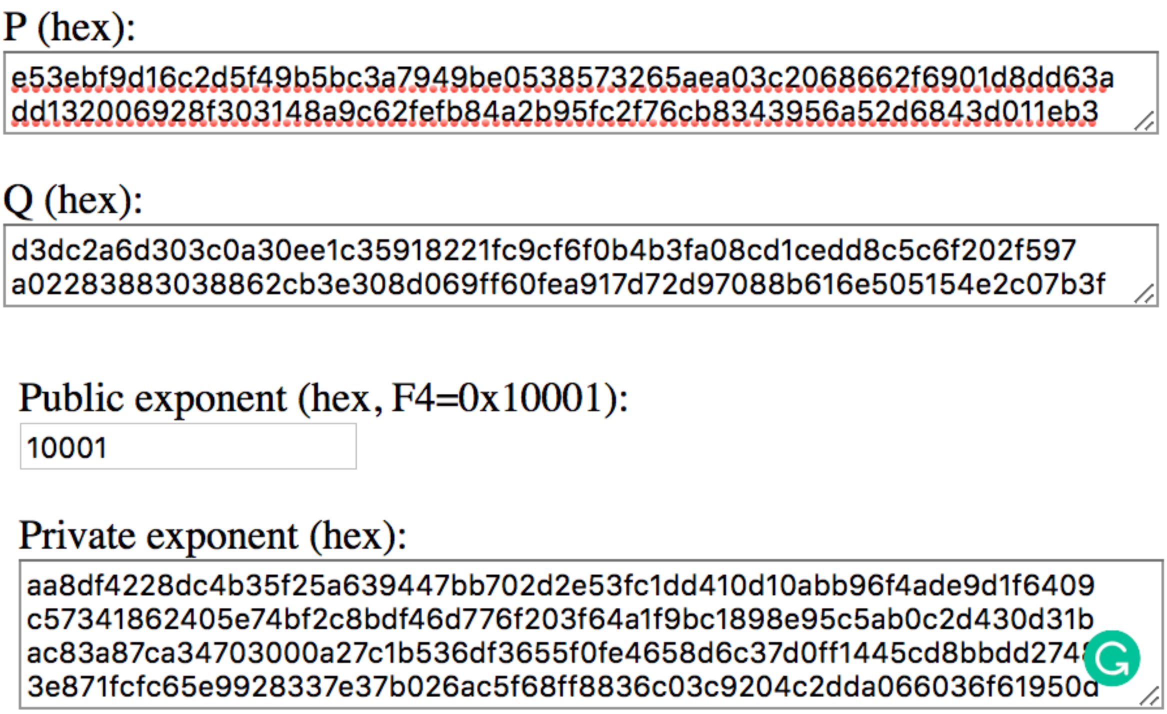
Question table:

Profile:	s3613252
AES key:	0123456712345678234567893456789a0123456712345678234567893456789a

p (hex):	e53ebf9d16c2d5f49b5bc3a7949be0538573265aea03c2068662f6901d8dd63a dd132006928f303148a9c62fefb84a2b95fc2f76cb8343956a52d6843d011eb3
q (hex):	d3dc2a6d303c0a30ee1c35918221fc9cf6f0b4b3fa08cd1cedd8c5c6f202f597 a02283883038862cb3e308d069ff60fea917d72d97088b616e505154e2c07b3f
Public exponent e (hex):	10001 (F4)
Private exponent d (hex):	aa8df4228dc4b35f25a639447bb702d2e53fc1dd410d10abb96f4ade9d1f6409 c57341862405e74bf2c8bdf46d776f203f64a1f9bc1898e95c5ab0c2d430d31b ac83a87ca34703000a27c1b536df3655f0fe4658d6c37d0ff1445cd8bbdd2748 3e871fcfc65e9928337e37b026ac5f68ff8836c03c9204c2dda066036f61950d
Encrypted AES key Encpk(K):	5e37a6e42df1e148641194f3bf74e5eaf170cf6b515fb9a7c55abd3f2e37f4ab a81e5400d9fc70bae9d909a2d997cc190ea861b511236ad9b1df7131ed8bfbdf fef0b8199409b3c69d609fce22ae1592a1bfaddbf58ccb4b63f96934473e414f c0a99ca6e7cc967038b09710f1a79645dddf9b115713afc3e4ee8b0af72a0588
Encrypted profile EncK(Profile):	7JQqYISMoI0cPXdLLLe2Yg==

RSA private key

1024 bit 1024 bit (e=3) 512 bit 512 bit (e=3) Generate bits = 1024



P (hex):

```
e53ebf9d16c2d5f49b5bc3a7949be0538573265aea03c2068662f6901d8dd63a
dd132006928f303148a9c62fefb84a2b95fc2f76cb8343956a52d6843d011eb3
```

Q (hex):

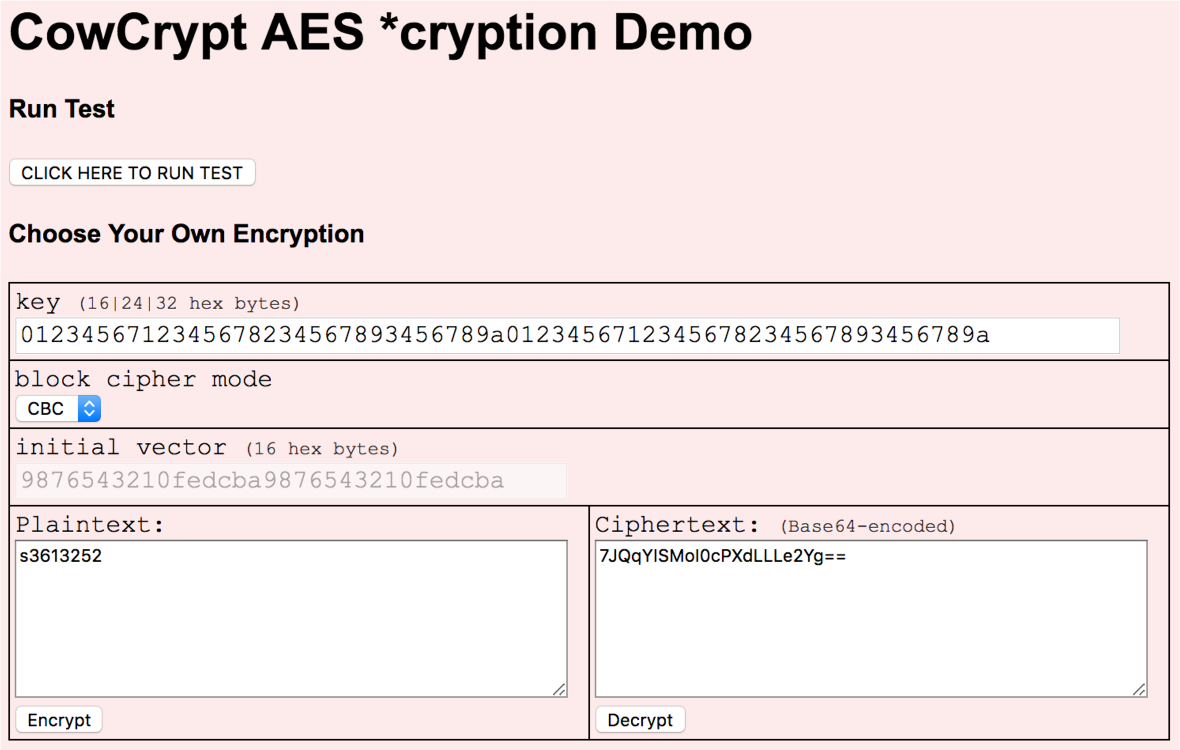
```
d3dc2a6d303c0a30ee1c35918221fc9cf6f0b4b3fa08cd1cedd8c5c6f202f597
a02283883038862cb3e308d069ff60fea917d72d97088b616e505154e2c07b3f
```

Public exponent (hex, F4=0x10001):

```
10001
```

Private exponent (hex):

```
aa8df4228dc4b35f25a639447bb702d2e53fc1dd410d10abb96f4ade9d1f6409
c57341862405e74bf2c8bdf46d776f203f64a1f9bc1898e95c5ab0c2d430d31b
ac83a87ca34703000a27c1b536df3655f0fe4658d6c37d0ff1445cd8bbdd274
3e871fcfc65e9928337e37b026ac5f68ff8836c03c9204c2dda066036f61950d
```



CowCrypt AES *cryption Demo

Run Test

Choose Your Own Encryption

key (16|24|32 hex bytes)

```
0123456712345678234567893456789a0123456712345678234567893456789a
```

block cipher mode: CBC

initial vector (16 hex bytes)

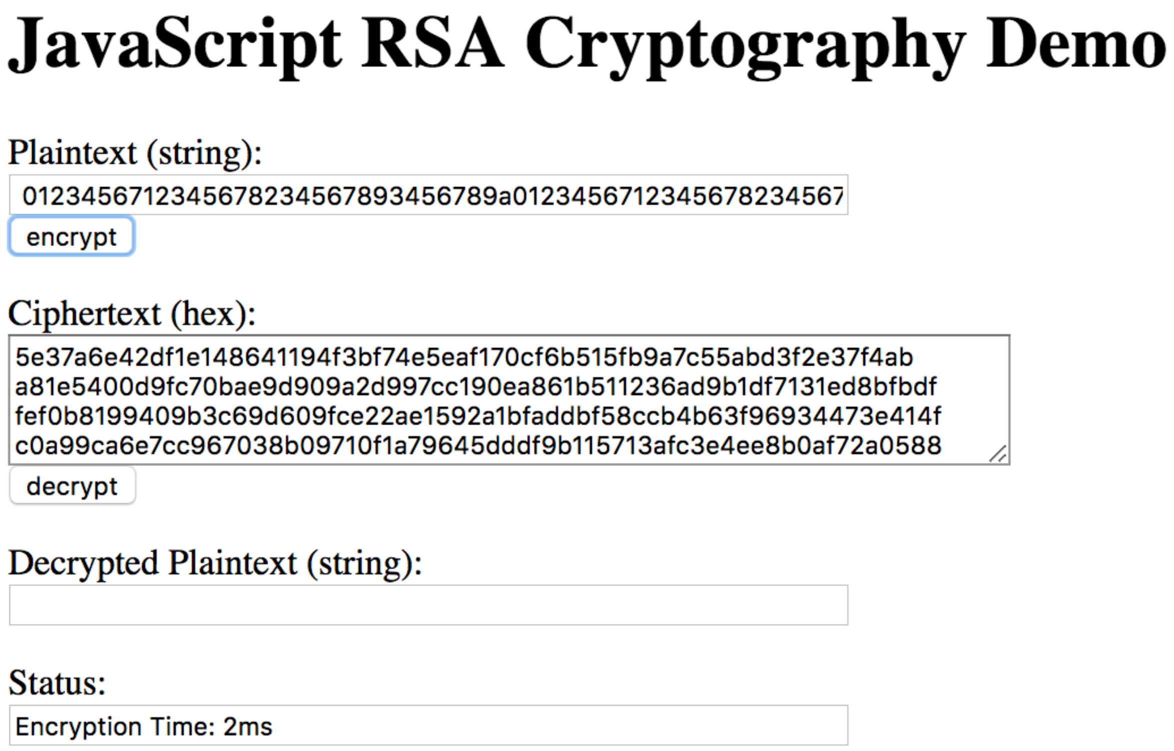
```
9876543210fedcba9876543210fedcba
```

Plaintext:

```
s3613252
```

Ciphertext: (Base64-encoded)

```
7JQqYISMol0cPXdLLLe2Yg==
```



JavaScript RSA Cryptography Demo

Plaintext (string):

```
0123456712345678234567893456789a0123456712345678234567
```

Ciphertext (hex):

```
5e37a6e42df1e148641194f3bf74e5eaf170cf6b515fb9a7c55abd3f2e37f4ab
a81e5400d9fc70bae9d909a2d997cc190ea861b511236ad9b1df7131ed8bfbdf
fef0b8199409b3c69d609fce22ae1592a1bfaddbf58ccb4b63f96934473e414f
c0a99ca6e7cc967038b09710f1a79645dddf9b115713afc3e4ee8b0af72a0588
```

Decrypted Plaintext (string):

Status:

```
Encryption Time: 2ms
```