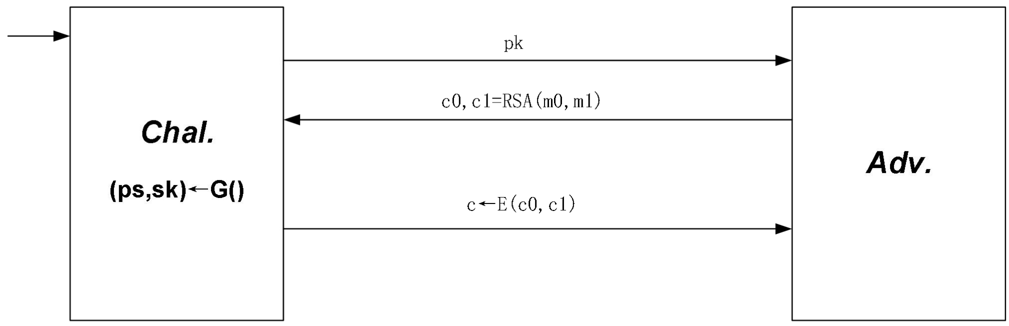
1.



First, Challenger B uses G() to generate A pair of public key pk and private key sk, and sends the public key to attacker A. The attacker then encrypts two messages, m0 and m1. Send the encrypted c0 and c1 to Challenger B. Because Challenger B has a private key, m0=c0, m1=c1. Challenger B can fully resolve messages sent by attacker A, so using RSA is semantically insecure.

2.

(a)

$$c_1 = mg_1^{S_1} (\bmod N)$$
$$x \equiv c_1 (\bmod p)$$
$$\therefore x = c_1 \equiv mg_1^{S_1} \equiv mg^{s_1 r_1 q(p-1)} \equiv m (\bmod p)$$
$$x = c_2 \equiv m(\bmod q)$$

Similarly, $x = c_2 \equiv m(\bmod q)$

So, Alice’s solution x is equal to Bob’s plaintext m.

x=m mod p①
x=m mod q②
由①x=m+py带入②
m+py=m mod q消掉m
py = 0 mod q
p^(-1)p · y=p^(-1) · 0 ->y=0 mod q
x=m+py
->x=m mod p,q