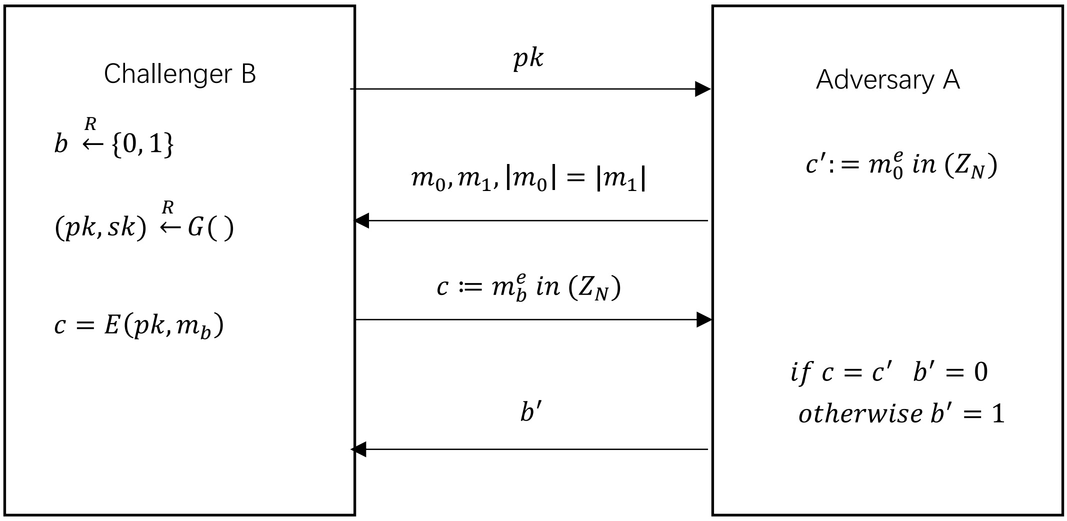
1. Textbook RSA (E, D):

$$E(pk, m) \coloneqq m^e \ in\ (Z_N); D(sk, c) \coloneqq c^d \ in\ (Z_N)$$

$$(pk, sk) \stackrel{R}{\leftarrow} G(\,), pk: (N, e), sk: (N, d)$$



Textbook RSA is **deterministic**. The ciphertext will be uniquely determined when the plaintext and public key are determined. Therefore, after adversary A obtains the $pk(N, e)$, he can encrypt the plaintext first, and then compare his ciphertext with the ciphertext encrypted by the challenger B.

Adversary A can completely distinguish EXP 0 and EXP 1,

$$Adv_{SS}[A, E] = |\Pr[EXP(0) = 1] - \Pr[EXP(1) = 1]| = 1$$

The encryption is not semantically secure.

2. a). **Prove:**

$$x \equiv c_1(mod\ p) \equiv mg_1^{s_1}(mod\ p) \equiv mg^{s_1 r_1 (p-1)}(mod\ p)$$

and

$$x \equiv c_2(mod\ q) \equiv mg_2^{s_2}(mod\ q) \equiv mg^{s_2 r_2 (q-1)}(mod\ q)$$

From Fermat's theorem, then

$$g^{p-1} \equiv 1(mod\ p)$$
$$g^{q-1} \equiv 1(mod\ q)$$
$$\therefore x \equiv m(mod\ p)\ and\ x \equiv m(mod\ q)$$

From Chinese Reminder Theorem, then

$$x = m + py, \quad y \in \mathbb{Z}$$
$$m + py \equiv m(mod\ p)$$
$$\therefore y = q$$
$$x = m + pq(mod\ pq) = m$$

Thus, Alice's solution x is equal to Bob's plaintext m.

b). **Analysis:**

From the description of the question, we know the public key is $pk(g_1, g_2, N)$ and the secret key is $sk(p, q)$.

$$g_1 = g^{r_1(p-1)}(mod\ N)$$
$$g_2 = g^{r_2(q-1)}(mod\ N)$$

From Fermat's Theorem, then

$$g_1 \equiv 1(mod\ p)$$
$$g_2 \equiv 1(mod\ q)$$

Which is also expressed as

$$g_1 - 1 \equiv 0(mod\ p)$$
$$g_2 - 1 \equiv 0(mod\ q)$$

Therefore, $(g_1 - 1)$ and N share a common factor p, $(g_2 - 1)$ and N share a common factor q. **Based on the above analysis, I give the following attack.**

My attack:

- Get public key $pk(g_1, g_2, N)$.
- Compute $gcd(g_1 - 1, N)$ to obtain p.
- Compute N/p to obtain q.
- Get secret key $sk(p, q)$.

This encryption can be easily broken by the attack I gave above.