Exercise 7

5130379092 谢尧

1. PayTV systems require that only the paid customers can watch the program, which of the 5 security services can be used to achieve this goal?

SOLUTION:

- Authentication is used to assure that the customers is the one who has paid.
- Access control is used to determine whether the customers can watch the program or not.
- Data integrity is used to make sure no customers can modify the access level to gain access without paying.

2. Determine the complexity (number of arithmetic operations) of
   a) computing gcd(a,b);
   b) computing RSA encryption $C=M^e \bmod n$

SOLUTION:

a) If a>2b, for a'=b and b'=a%b, a' will be less than half a. If a<=2b, b' will be less than half b. Thus, every step will decrease one of the parameter by at least half the previous value. The complexity is $O(\log_2(a)+\log_2(b))$.

b) Considering the square-multiplication algorithm for RSA encryption, every multiplication operation needs $O(k^2)$ complexity where k is the text length and the algorithm needs log(e) multiplications. Thus, the complexity is $O(\log(e)*k^2)$.

3. Limitation of raw RSA signature: Only when M has redundancy structure, can the signature be securely verified. Why?

SOLUTION:

If M doesn't have redundancy structure, it is susceptible to existential forgeries. Let (e,N) be the public signature verification key of RSA, then one can randomly choose a signature σ and compute the message $m\equiv\sigma^e \pmod N$. Applying a redundancy structure to messages, for example, hashing and padding prior to signing, the forged signatures would be useless so that the signature can be securely verified.

4. For RSA, it requires |p-q| should not be small. Task: design an attack if |p-q| is smaller than 10000.

SOLUTION:

Since |p-q| is smaller than 10000, using this as a constraint, n can be easily factorized. After getting p and q, the totient of the product can be computed. Then for public key exponent e, the corresponding private key exponent d can be calculated. In this way, RSA can be broken in the limited time.

5. Show that in RSA, knowing Φ(n) is equivalent to knowing the factorization of n.

PROOF:

It is known that n=pq and Φ(n)=(p-1)(q-1), so we can write the equation as follows

$$\Phi(n)=(p-1)(q-1)=pq-p-q+1=n-(p+q-1).$$

In this way, by calculating n-Φ(n)+1, we get the sum of p and q. Then from the knowing of n=pq, n-Φ(n)+1=p+q and p, q are all prime numbers, we can easily calculate the values of p and q. Therefore, we know the factorization of n.