Homework 3

Pan Yisheng
515021910384

March 28, 2018

Problem 1. RSA Assume that we use RSA with the prime numbers p = 17 and q = 23.

a) Calculate $n = pq$ and $\phi(n)$.

b) Given the public exponent $e = 7$, calculate d.

c) Calculate the ciphertext of the message $M = 15$.

d) Calculate the plaintext of the ciphertext $C = 31$.

Solution a):

$$n = pq = 17 \times 23 = 391, (n) = (p-1)(q-1) = 16 \times 22 = 352.$$

b):We can calculate d using extended Euclidean algorithm.

$$352 = 7 \times 50 + 2 \rightarrow 1 = 7 \times 151 - 352 \times 3$$
$$7 = 2 \times 3 + 1 \rightarrow 1 = 7 - 2 \times 3$$

Therefore,

$$d = e^{-1} \mod \phi(n) = 151$$

c):

$$C = M^e \mod n = 15^7 \mod 391 = 195$$

d):

$$M = C^d \mod n = 31^{151} \mod n = 142$$

Problem 2. Breaking RSA In RSA, n and e are public, while d is private. It turns out that $\phi(n)$ also has to remain private. Show that given n and $\phi(n)$ it is possible to calculate p and q.

Solution Using Euler phi Function,we can get

$$\phi(n) = (p-1)(q-1)$$

Therefore,

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

Then we can calculate q and q,

$$\begin{cases} p+q = n-\phi(n)+1 \\ pq = n \end{cases} \rightarrow \begin{cases} p = \frac{1+n-\phi(n)+\sqrt{(1+n-\phi(n))^2-4n}}{2} \\ q = \frac{1+n-\phi(n)-\sqrt{(1+n-\phi(n))^2-4n}}{2} \end{cases}$$

Problem 3. El-Gamal Consider the El-Gamal encryption scheme and let $p = 13$ and $g = 7$.

a) Assume the private key is $x = 5$. Compute the public key y.

b) Encrypt the message $M = 10$ using the public key above and $r = 3$.

c) Verify that the encryption in 3b worked by decrypting the calculated ciphertext.

d) Assuming you got the ciphertext $C = (A, B)$ in 3b, modify it to $C = (A, 2B)$ (remember it is still mod 13) and try to decrypt C.

Solution a): We can calculate the public key:

$$y = g^x \ mod \ p = 7^5 \ mod \ 13 = 11$$

b): We compute,

$$A = g^r \equiv 7^3 \equiv 5 \ (mod \ 13)$$

$$B = My^r \equiv 10 \times 11^3 \equiv 11 \ (mod \ 13)$$

Therefore, the ciphertext $C = (A, B) = (5, 11)$.
c): For decryption, we compute

$$K = A^x \equiv 5^5 \equiv 5 \ (mod \ 13)$$

$$M = BK^{-1} \equiv 11 \times 5^{-1} \equiv 11 \times 8 \equiv 10 \ (mod \ 13)$$

d): We modify the ciphertext to $C' = (A, 2B) = (5, 9)$

$$M' = B'K^{-1} \equiv= 9 \times 8 \equiv 7 \ (mod \ 13)$$

Problem 4. Diffie-Hellman Consider a Diffie-Hellman key exchange with $p = 17$ and $g = 11$.

a) Alice picks $x = 5$, what is the public A she will send to Bob?

b) Bob picks $y = 9$, what is the public B he will send to Alice?

c) What is the shared key K resulting from the exchange?

d) Assume Trudy intercepts the key exchange and uses her own private value $t = 3$. Calculate the keys shared between Alice and Trudy as well as Trudy and Bob.

e) If Alice and Bob communicate over the Internet, for example, will they be aware of the fact that Trudy is in the middle, intercepting the key exchange?

Solution a): We can compute public A,

$$A = g^a \equiv 11^5 \equiv 10 \ (mod\ 17)$$

b): We can compute public B,

$$B = g^b \equiv 11^9 \equiv 6 \ (mod\ 17)$$

c): We can compute the shared key K,

$$K = A^b = B^a \equiv 6^5 \equiv 7 \ (mod\ 17)$$

d):We can get,

$$K_{Alice-Trudy} = A^t \equiv 10^3 \equiv 14 \ (mod\ 17)$$
$$K_{Bob-Trudy} = B^t \equiv 6^3 \equiv 12 \ (mod\ 17)$$

e): No, they can't know Trudy is in the middle.The attack is also called *Man-in-the-Middle Attack*.

Problem 5. RSA Signature Assume we are using an RSA signature scheme with $n = pq$,private key d, public key e, where the signature is calculated as $S = M^d \bmod n$ and can be verified by checking $S^e \bmod n = M$.
Unfortunately, this signature scheme only works when M is smaller than n. We therefore decide to split a large message M into several parts, each smaller than n. For example a message M might be split into three parts,$M = M1||M2||M3$ (where||denotes concatenation). A signature is then calculated for each part individually, i.e.,

$$S_1 = M_1^d \ mod\ n$$

$$S_2 = M_2^d \ mod\ n$$
$$S_3 = M_3^d \ mod\ n$$

and the final signature becomes $S = S1||S2||S3$.

a) Show that in this scheme it is easy to forge a new message M and corresponding *valid* signature S from the given message M and signature S above without knowing d

b) Assume you are able to intercept and modify the electronic communication between two banks which sign their messages using the scheme described above to ensure that the instructions are genuine. When bank A transfers money from one of its accounts to an account of bank B, it sends the following message together with the signature:

$$M = Pay||1000\ RMB||to\ account||123456$$

$$S = S_1||S_2||S_3||S_4$$

Assume you have a bank account with both bank A and bank B. Find a way to get rich by intercepting and modifying the communication between the two banks.

Solution a): We can forge a new message M' by exchanging the position of sub message and modify the signature by exchanging the position of corresponding part of original signature .ie.

$$M' = M_3||M_2||M_1 \quad , S' = S_3||S_2||S_1$$

b):We can become rich by 3 steps:

1. By transfer some money from my bank A account to my bank B account, we can get the signature of my bank B account(S_4) .
2. By intercepting the communication between the two banks, we can get other's message $M'' = M_1''||M_2''||M_3''||M_4''$ and signature $S'' = S_1''||S_2''||S_3''||S''4$.
3. By modify the message and signature into $M_s = M_1''||M_2''||M_3''||MYID$ and $S'' = S_1''||S_2''||S_3''||S4$,we can transfer other people's money to my account.

Problem 6. Hash Function Assume prime $p = 13$ and a generator $g = 7$.

a) Find two distinct positive integers x and y such that:

$$g^x \ mod \ p = g^y \ mod \ p$$

b) Given the question 6a above, explain why $h(x) = g^x \bmod p$ is not a good hash function.

c) Does the hash function $h(x) = g^x \bmod p$ satisfy one-wayness?

Solution a): We can find that x and y have the relationship:

$$y - x = 12 \times n, n = 1, 2, ...$$

b): Even if the prime p is large,we can easily break compromise collision resistance by trying p times.

c): The hash function $h(x) = g^x \ mod \ p$ satisfy one-wayness. Because we can't break Discrete Logarithm now.