Network Security Technology Spring, 2019
Tutorial 3, Week 4 (March 20) LIU Zhen
Due Date: March 27

Questions:

1. **RSA (20 Points)** Assume that we use RSA Encryption with the prime numbers $p = 19$ 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) We have $n = pq = 437$. We know that p and q are prime and therefore $\phi(n) = \phi(pq) = (p-1) \cdot (q-1) = 396$.
   (b) We use the extended Euclidean algorithm to obtain $d = 283$, such that $e \cdot d = 1 \mod 396$.
   (c) The ciphertext is calculated as $C = M^e \mod n = 15^7 \mod 437 = 241$.
   (d) The plaintext is calculated as $M = C^d \mod n = 31^{283} \mod 437 = 50$.

2. **RSA (15 Points)** In RSA Encryption, let the public key is (n, e), and the private key is d. To encrypt a message $M \in Z_n$, the cipherytext is $C = M^e \bmod n$. To Decrypt a ciphetext $C \in Z_n$, the plaintext is computed as $M = C^d \bmod n$.
   (a) Check the correctness, i.e. whether for any message $M \in Z_n$, $M \stackrel{?}{=} (M^e \bmod n)^d \bmod n$ holds.
   (b) Let $M \in Z_n$ be a uniformly random message. Compute the probability that $gcd(M, n) \neq 1$.

   Solution

   (a) $(M^e \mod n)^d \bmod n = M^{ed} \bmod n$
   We already have $ed \equiv 1 \bmod \phi(n)$

   If M and n are relatively-prime,
   then $M^{ed} \mod n = M^1 \cdot M^{k \cdot \phi(n)} \bmod n = M \bmod n$. (Euler Theorem)

   If M and n are not relatively-prime, suppose $M = k \cdot p$, M and q are relatively-prime.
   We have $M^{\phi(q)} \equiv 1 \bmod q$, then:

$$\begin{aligned} M^{k\phi(p)\phi(q)} &\equiv 1 \bmod q \\ M^{k\phi(n)} &\equiv 1 \bmod q \\ M^{k\phi(n)} &= 1 + r \cdot q \\ M^{k\phi(n)+1} &= kp + kprq = M + kr \cdot n \\ M^{ed} &\equiv M \bmod n \end{aligned}$$

Therefore, $M = (M^e \bmod n)^d \bmod n$

(b) Since $M \in Z_n$ is a uniformly random message and there are $\phi(n)$ messages in Z_n that $gcd(M, n) = 1$, the probability that $gcd(M, n) \neq 1$ is $\frac{p+q-1}{p \cdot q}$

3. **Breaking RSA (10 Points)** In RSA Encryption, 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 From the definition of $\phi(n)$ we have the following equation:

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

Transforming the equation we get:

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

From the equation $n = p \cdot q$ we also have the know that:

$$p = \frac{n}{q}$$

Combining these two equations we get:

$$\frac{n}{q} = n - \phi(n) - q + 1$$

Finally resulting in:

$$q^2 - q(n - \phi(n) + 1) + n = 0$$

This is a quadratic equation, which can be solved using the usual formula, and we get:

$$p \text{ or } q = \frac{(n - \phi(n) + 1) \pm \sqrt{(n - \phi(n) + 1)^2 - 4n}}{2}$$

4. **El-Gamal (20 Points)** Consider the El-Gamal encryption scheme and let $p = 17$ 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 4b worked by decrypting the calculated ciphertext.

(d) Assuming you got the ciphertext $C = (A, B)$ in 4b, modify it to $C' = (A, 2B)$ (remember it is still $\bmod 17$) and try to decrypt C'.

Solution

(a) The public key is calculated as $y = g^x \bmod p$. In this case we have $y = 7^5 \bmod 17 = 11$.

(b) First we choose a random $r \in \mathbb{Z}_{16}$, $r = 3$ in this case as indicated. We then calculate:

$$A = g^r \bmod p = 7^3 \bmod 17 = 3$$
$$B = M \cdot y^r \bmod p = 10 \cdot 11^3 \bmod 17 = 16$$

And the ciphertext is $C = (A, B) = (3, 16)$.

(c) Decryption involves two steps:

$$K = A^x \mod p = 3^5 \mod 17 = 5$$
$$M = B \cdot K^{-1} \mod p = 16 \cdot 5^{-1} \mod p = 16 \cdot 7 \mod 17 = 10$$

And we can successfully recover the original paintext.

(d) We have $C' = (3, 15)$. Decrypting C' yields:

$$K = A^x \mod p = 3^5 \mod 17 = 5$$
$$M = B \cdot K^{-1} \mod p = 15 \cdot 5^{-1} \mod p = 15 \cdot 7 \mod 17 = 3$$

We can see that $M' = 3 = 2 \cdot 10 \mod 17 = 2 \cdot M \mod 17$. El-Gamal is in fact *malleable*, that means modifying the ciphertext leads to a predictable change in the decrypted plaintext (i.e., changing $C = (A, B)$ to $C' = (A, 2B)$ will lead to $M' = 2M$ upon decryption).

5. **Diffie-Hellman (15 Points)** 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) Alice calculates:

$$A = g^x \mod p = 11^5 \mod 17 = 10$$

and sends $A = 4$ to Bob.

(b) Bob calculates:

$$B = g^y \mod p = 11^9 \mod 17 = 6$$

and sends $B = 6$ to Alice.

(c) Both Alice and Bob can calculate the shared key, with Alice calculating:

$$K = B^x \mod p = 6^5 \mod 17 = 7$$

and Bob calculating:

$$K = A^y \mod p = 10^9 \mod 17 = 7$$

and we can thus see that they both arrive at the same result $K = 7$.

In reality, the numbers used would be much larger, and the output K is not normally used directly as the key, but used as the input to a *key derivation function* which then outputs the actual key to use.

(d) Trudy's public value is:

$$T = g^t \mod p = 11^3 \mod 17 = 5$$

Which will result in the following key being shared between Alice and Trudy:

$$K_{\text{Alice}} = T^x \mod p = 5^5 \mod 17 = 14$$

and another key being shared between Trudy and Bob:

$$K_{\text{Bob}} = T^y \mod p = 5^9 \mod 17 = 12$$

(e) No, Alice and Bob are unaware of the fact that the key exchange is compromised. Unless they authenticate the exchanged values A and B through other means, they cannot detect Trudy.

6. **RSA Signature (20 Points)** Assume we are using an RSA signature scheme with $n = pq$, private key d, public key e, where the signature is calculated as $S = M^d \mod n$ and can be verified by checking $S^e \mod n = M$.

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, $M = M_1||M_2||M_3$ (where $||$ denotes concatenation). A signature is then calculated for each part individually, i.e.,

$$\begin{aligned} S_1 &= M_1^d \mod n \\ S_2 &= M_2^d \mod n \\ S_3 &= M_3^d \mod n \end{aligned}$$

and the final signature becomes $S = S_1||S_2||S_3$.

(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:

$$\begin{aligned} M &= \text{Pay} \;||\; \text{1000 RMB} \;||\; \text{to account} \;||\; \text{123456} \\ S &= S_1||S_2||S_3||S_4 \end{aligned}$$

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) It turns out that because each part in the message has a corresponding part in the signature, one can easily change the message by rearranging parts and ensure that the signature is still valid by rearranging the corresponding parts in the signature as well. For example, from $M = M_1||M_2||M_3$ we can create $M' = M_1||M_3||M_2$ (exchange M_2 and M_3) and then do the same rearranging in the signature $S' = S_1||S_3||S_2$. S' is now a valid signature for the newly created message M'.

(b) First, you wait for somebody to make a transfer from bank A to bank B with a large amount and record the message and the corresponding signature. Assume the message and signature recorded are as shown above (i.e., 1000 RMB to account 123456). Then, you make a small transfer from your account in bank A to your account in bank B, say 1 RMB. You wait for the instruction to arrive on the communication link and intercept it:

$$M' = \text{Pay} \;||\; 1 \text{ RMB} \;||\; \text{to account} \;||\; 111111$$
$$S' = S'_1||S'_2||S'_3||S'_4$$

You then change the message to read

$$M'' = \text{Pay} \;||\; 1000 \text{ RMB} \;||\; \text{to account} \;||\; 111111$$

and update the signature by replacing the S'_2 with the signature part S_2 from the previously recorded message:

$$S'' = S'_1||S_2||S'_3||S'_4$$

You then forward the modified message M'' together with the modified (valid) signature S''. Your account in bank A now contains 1 RMB less, but you gained 1000 RMB on your account in bank B.

Rest assured that banks use better security than this, though.