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 $C = 31$.

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 $M \in Z_n$, $M \overset{?}{=} (M^e \bmod n)^d \bmod n$ holds.
   (b) Let $M \in Z_n$ be a uniformly random message. Compute the probability that $gcd(M, n) \neq 1$.

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.

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'.

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?

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.