CS 478/513: Computer Security

Written Assignment 3
Due: 4/25/22, 11:59 pm
Total points: 100

Please complete the following problems, being sure to explain your conclusions and show your work for all problems. Your solutions must be submitted to Canvas as a PDF file.

This assignment is to be completed individually — plagiarism and cheating are strictly prohibited and are punishable.

Chapter 4:

1. (15 points) This question relates to the Diffie-Hellman secret exchange mechanism. Suppose that Alice and Bob want to derive a shared key and have agreed on a prime $p = 17$ and generator $g = 3$. Alice's private exponent $a = 9$ and Bob's private exponent $b = 5$.

   (a) Alice sends Bob $g^a \bmod p$, and Bob sends Alice $g^b \bmod p$. Show the computation of each of these values.

   $g^a \bmod p = 3^9 \bmod 17$. Let us use the repeated squares method. We can decompose 3^9 into $3^{8+1} = 3^8 \cdot 3^1$. Let us calculate the values of these components: $3^1 \bmod 17 = 3$; $3^2 \bmod 17 = 9$; $3^4 \bmod 17 = 9^2 \bmod 17 = 13$; $3^8 \bmod 17 = 13^2 \bmod 17 = 16$. Now, we substitute: $3^9 \bmod 17 = (3^8 \cdot 3^1) \bmod 17 = (16 \cdot 3) \bmod 17 = 14$. Therefore, Alice sends Bob the value 14.

   Computation of $g^b \bmod p = 3^5 \bmod 17$ is similar. The computation is omitted here, but the result is 5. This is the value that Bob sends to Alice.

   (b) Show that Alice and Bob will both obtain the same shared secret from the transmitted values. Compute that secret.

   Bob calculates $(g^a)^b \bmod p = 14^5 \bmod 17 = 12$.

   Alice calculates $(g^b)^a \bmod p = 5^9 \bmod 17 = 12$.

   (c) Suppose that Trudy attempts a Man-in-the-Middle attack on Alice and Bob's key exchange. Trudy has private exponent $t = 7$. Show the process of the attack. Show the values that Trudy sends to Alice and Bob, and compute the shared secrets that she establishes with each of them. Trudy intercepts the transmissions of $g^a \bmod p$ and $g^b \bmod p$ from Alice and Bob respectively. She then sends her own share, $g^t \bmod p = 3^7 \bmod 17 = 11$ to each of them. Trudy computes $(g^a)^t \bmod p = 14^7 \bmod 17 = 6$ as her shared secret with Alice, and computes $(g^b)^t \bmod p = 5^7 \bmod 17 = 10$ as her shared secret with Bob. Alice and Bob will derive the same shared secrets by computing $(g^t)^a \bmod p$ and $(g^t)^b \bmod p$ respectively.

2. (10 points) This question concerns the RSA asymmetric cipher. Suppose Bob uses $e = 7$ and $N = 221$ for his public key.

   (a) Bob wants to encrypt the plaintext $M = 2$ with his public key. What vulnerability is the ciphertext susceptible to? Demonstrate that Trudy can recover the plaintext without Bob's private key.

   This message is vulnerable to the cube-root attack. Bob will compute $M^e \bmod N = 2^7 \bmod 221 = 128$. Then Trudy can calculate $128^{(1/7)} = 2$ and recover the message.

   (b) The security of RSA is derived from the difficulty of factoring large numbers. In this case, N is relatively small. Factor N into the primes p and q, and find Bob's private exponent d.

   Factoring N, we obtain $p = 13$ and $q = 17$. Then, we find d such that $de \equiv 1 \pmod{\phi(N)}$. The solution is $d = 55$.

3. (10 points) Textbook problem 7.

   If Alice encrypts a message M, $M^e mod N \rightarrow C$, then an adversary can ask her to produce a signature on C. She will do $C^d modN \rightarrow M$. Hence an adversary can get decryption of any message by just asking for a signature on it. Of course Alice needs to be willing to produce the signature though.

Another reason is if d gets compromised, not only will all previously encrypted messages become decryptable, but the authenticity of all previously produced signatures will be doubtful.

Chapter 7:

4. (21 points) Complete Problem 7 (a, b, c) from the textbook.

   (a) There is a 1/4 chance that Alice's password exists in Trudy's dictionary, and a 3/4 chance that Trudy will have to bruteforce it. The amount of work required to iterate through the dictionary is $2^{30}/2$, and the amount of work required to bruteforce is $2^{56}/2$. Therefore, the overall expected workload is $1/4 \cdot (2^{29}) + 3/4 \cdot (2^{55}) \approx 2^{55}$.

   Had Trudy precomputed the hashes of every password, the work to look up a hash in the dictionary would be negligible, in which case the effective amount of work would only be $3/4 \cdot (2^{55})$.

   (b) The work is the same, since Trudy is targeting a single password. However, precomputing the hashes would no longer give her an advantage.

   (c) Each password has a 1/4 chance of being in the dictionary; therefore it has a 3/4 chance of not being in the dictionary. So, the probability that none of the 2^{10} passwords are in the dictionary is $(3/4)^{2^{10}} \approx 2^{-425}$. Then the probability that at least password is in the dictionary is very close to 1; i.e., it is almost certain.

5. (24 points) Complete Problem 10 (a, b, c, d) from the textbook.

   (a) There are $64^8 = 2^{48}$ unique passwords.

   (b) To target one password, the number of hashes Trudy must calculate is $1/4 \cdot 2^{30-1} + 3/4 \cdot 2^{48-1} \approx 2^{47}$.

   (c) The probability that at least one password is in the dictionary is $1 - (3/4)^{256} \approx 1$; i.e., it is almost certain.

   (d) Since the passwords are salted, Trudy does not have the option to precompute hashes; she must either resort to using the attack in part (b) by targeting a specific password, or choose to attempt to only compute the dictionary hashes for each salt. Using this second method, she would expect to find one dictionary password after testing two; therefore she would compute about $2 \cdot 2^{30}$ hashes.

6. (20 points) Complete Problem 26 (a, b) from the textbook.

   (a) Each of the 10^5 fingerprints will be compared against 10^7, and there will be a 10^{-10} chance of a false positive each time; therefore, we would expect $10^5(1 - (1 - 10^{-10})^{10^7}) \approx 100$ false positives overall.

   (b) Each suspect will have a false match with probability $1 - (1 - 10^{-10})^{10^7} \approx 0.001$.