CS 4920/5920 Spring 2022

HW 5

This HW is due on 5/6. Explain how you reached your answers. Answers without explanations will receive no to little credit.

Problem 1.

Perform encryption and decryption using the RSA algorithm, as in Figure 9.5, for the following:

a. $p = 3$; $q = 11$, $e = 7$; $M = 5$
b. $p = 7$; $q = 11$, $e = 17$; $M = 8$
c. $p = 11$; $q = 13$, $e = 9$; $M = 7$
d. $p = 17$; $q = 31$, $e = 7$; $M = 2$

Problem 2.

a. In a public-key system using RSA, you intercept the ciphertext $C = 10$ sent to a user whose public key is $e = 5$, $n = 35$. What is the plaintext M?

b. In a RSA system, the public key of a given user is $e = 31$, $n = 3599$. What is the private key of this user? *Hint*: First use trial-and-error to determine p and q; then use the extended Euclidean algorithm to find the multiplicative inverse of 31 modulo $\varphi(n)$.

c. Use the fast exponentiation algorithm of Figure 9.8 to determine 5^{596} mod 1234. Show the steps involved in the computation by identifying the c and f values over the iterations across i.

Problem 3.

Users A and B use the Diffie-Hellman key exchange scheme with a common prime $q = 71$ and a primitive root $a = 7$.

a. If user A has private key $X_A = 4$, what is A's public key Y_A?
b. If user B has private key $X_B = 11$, what is B's public key Y_B?
c. What is the shared secret key?

Now consider a Diffie-Hellman scheme with a common prime $q = 11$ and a primitive root $a = 2$.

d. Show that 2 is a primitive root of 11.
e. If user A has public key $Y_A = 9$, what is A's private key X_A?
f. If user B has public key $Y_B = 3$, what is the secret key K shared with A?
g. If attacker E has both public keys Y_A and Y_B, can it also know K? Explain why or why not.
h. If attacker E has both public keys Y_A and Y_B, can it launch man-in-the-middle attack? Explain why or why not.

Problem 4.

a. Suppose H(m) is a collision-resistant hash function that maps a message of arbitrary bit length into an n-bit hash value. Is it true that, for all messages x, x' with $x \neq x'$, we have $H(x) \neq H(x')$? Explain your answer.

b. Define weak collision resistance (second preimage resistance) and strong collision resistance and explain how they are different.

c. Let's use an encryption algorithm to construct a one-way hash function. Consider using RSA with a known key. Then process a message consisting of a sequence of blocks as follows: encrypt the first block, XOR the result with the second block and encrypt again, and so on.

Show that this scheme is not secure by solving the following problem. You are given a two-block message B1, B2, and its hash:

$$\text{RSAH (B1, B2)} = \text{RSA (RSA(B1)} \oplus \text{B2)}$$

First, given an arbitrary block D1, choose D2 so that RSAH (D1, D2) = RSAH (B1, B2). Second, what is the security issue for using this hash function for cryptographic applications?

Problem 5.

The following problems are about SHA-512.

a. In Figure 11.12, it is assumed that an array of 80 64-bit words is available to store the values of W_t, so that they can be precomputed at the beginning of the processing of a block. Now assume that space is at a premium. As an alternative, consider the use of a 16-word circular buffer that is initially loaded with W_0 through W_{15}. Design an algorithm that, for each step t, computes the required input value W_t.

b. For SHA-512, show the equations for the values of W_{16}, W_{17}, W_{18}, and W_{19}. Define and explain the variables you use.

Problem 6.

a. The data authentication algorithm, described in Section 12.6 ("MACs Based on Block Ciphers: DAA and CMAC"), can be defined as using the cipher block chaining (CBC) mode of operation of DES with an initialization vector of zero (Figure 12.7). Show that the same result can be produced using the cipher feedback mode and identify the input parameters.

b. At the beginning of Section 12.6, it was noted that given the CBC MAC of a one-block message X, say $T = \text{MAC}(K,X)$, the adversary immediately knows the CBC MAC for the two-block message $X \| (X \oplus T)$ since this is once again T. Justify and explain this statement.