Worksheet 2 - CPA Security, MACs

October 18, 2022

1 Definitions

1.1 Chosen plaintext attack (CPA)

The adversary is given access to an encryption oracle $\mathsf{Enc}()$, which receives plaintexts m and outputs $c = \mathsf{Enc}(m)$.

To win the CPA game, the adversary constructs two messages m_0, m_1 such that $m_0 \neq m_1$ and is given one ciphertext c^* that corresponds to one of those messages. Adversary wins if he can distinguish which message corresponds to which c^* with greater than $\frac{1}{2}$ probability.

1.2 Message authentication code (MAC) security

The following is the security game for message authentication codes (MACs).

- The game master chooses a random MAC key k.
- The adversary has access to a $\mathsf{MAC}_k()$ oracle (but not k), that receives messages m chosen by the adversary and outputs $\mathsf{MAC}_k(m)$.
- The adversary has access to a verification oracle $\mathsf{Ver}_k()$, that receives a message m and a tag t chosen by the adversary. $\mathsf{Ver}_k()$ outputs 1 if t is a valid MAC on a message m.
- The adversary wins if she outputs m^*, t^* such that $\mathsf{Ver}_k(m^*, t^*) = 1$. Note that adversary *can not* previously query the $\mathsf{MAC}_k()$ oracle with m^*, t^*.

We say the MAC is secure if no (polynomial time) adversary can win this game with probability better than about $\frac{1}{2^\ell}$, where ℓ is the length of the MAC tag.

Exercise 1. In a Caesar cipher, each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet. For example, with a left shift of 3, D would be replaced by A, E would become B, and so on. The key is the number of positions used in the left shift. This cipher is named after Julius Caesar, who used it in his private correspondence.

1. Present an attack that proves that the Caesar's cipher is NOT CPA secure.

Exercise 2. Let E be any encryption scheme that takes in a key of length λ and message of length ℓ and produces ciphertexts of length ℓ'.

Assume that E is CPA secure. (E might be encryption in CBC mode, as discussed in class.)

Now let E' be an encryption scheme identical to E except with the following modification; the 3^{rd} bit in the ciphertext is equal to the 3^{rd} bit of the plaintext.

Show that E' is not CPA secure.

Exercise 3. Alice and Bob share a secret 128-bit key k that they will use to authenticate every message that they send.

Every time Alice wants to send a message m to Bob, she breaks the message m up into blocks $m_1, m_2, \ldots, m_n$ and outputs the tag for each block $t_1, t_2, \ldots, t_n$, where $t_i = \mathsf{MAC}_k(m_i, i)$ for all $i \in \{1, \ldots, n\}$.

Alice sends $m_1, m_2, \ldots, m_n$ and $t_1, t_2, \ldots, t_n$ to Bob.

1. Write down the verification algorithm for this scheme.

2. Prove that this scheme is not a secure MAC.

Exercise 4. An airline uses *manifests* to determine which passenger should be on which flight. The airline has the secret key k. Each manifest consists of:

- The flight number x and its date and time d
- A MAC $t = \mathsf{MAC}_k(x||d)$.
- The name of the 1st passenger p_1, and a MAC tag $t_1 = \mathsf{MAC}_{SK}(p_1)$.
- The name of the 2nd passenger p_2, and a MAC tag $t_2 = \mathsf{MAC}_{SK}(p_2)$.

  $\vdots$
- The name of the n-th passenger p_n, and a MAC tag $t_n = \mathsf{MAC}_{SK}(p_n)$.

Notice that n will be different for each flight.

The manifest is checked, using the key k, as passengers board the flight.

1. Suppose you can intercept and modify manifests before they arrive at each flight. Explain how you can travel to Tokyo for the cost of a flight to Chicago.
2. From now on, we modify the manifest to be
   - The flight number x and its date and time d
   - A value $h = H(x||d)$ where H is a collision-resistant hash.
   - The name of the 1st passenger p_1, and a MAC tag $t_n = \mathsf{MAC}_k(h||p_1)$.
   - The name of the 2nd passenger p_2, and a MAC tag $t_2 = \mathsf{MAC}_k(h||p_2)$.

     $\vdots$
   - The name of the n-th passenger p_n, and a MAC tag $t_n = \mathsf{MAC}_k(h||p_n)$.

   Notice that n will be different for each flight.
3. Explain why your attack from the previous part no longer works.
4. However, there is still something terrible about this scheme.
   The number of passengers on the flight, n, is never signed.
   Present an attack that demonstrate why this is a problem.