CIS4362.01 Homework 4 Due 12/6/19

Brandon Thompson 5517

December 4, 2019

1. Draw the schematic view of all MAC and Encryption combinations which are implemented by programmers for providing authenticated encryption. Which combination always provides authenticated encryption?

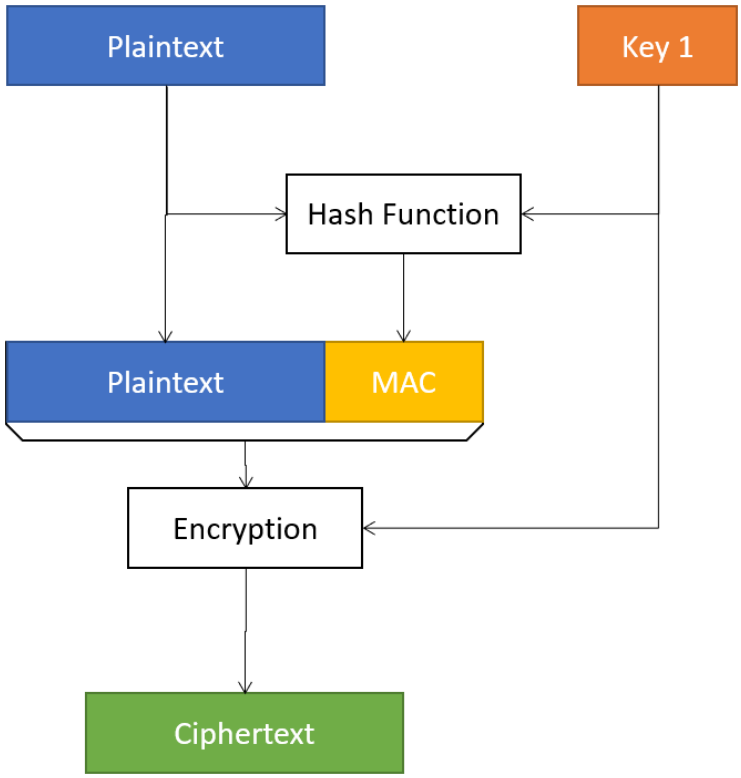

Figure 1: Mac-then-encrypt (SSL).

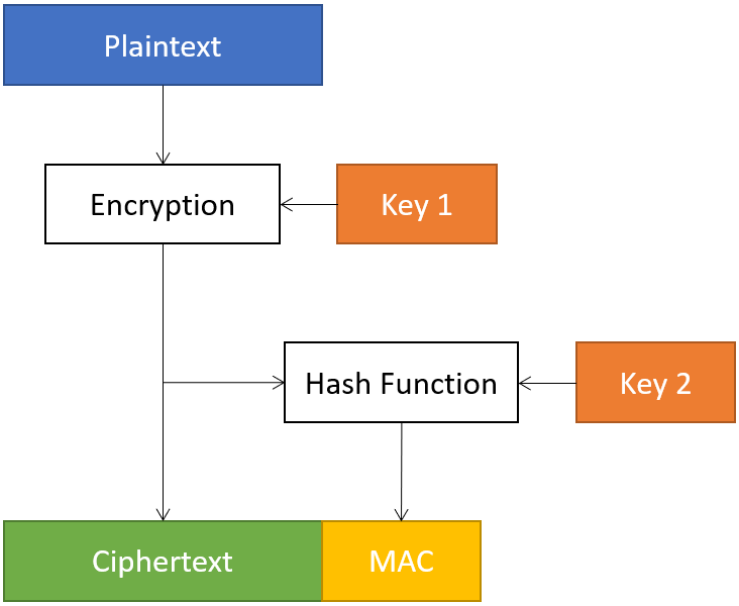

Figure 2: Encrypt-then-mac (IPsec). Always provides authenticated encryption.

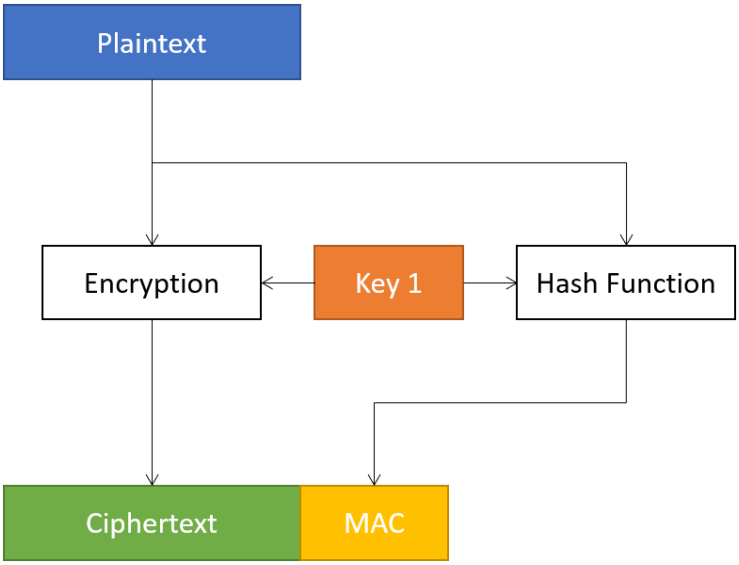

Figure 3: Encrypt-and-mac (SSH).

2. How a key be generated using Trusted 3rd Party (TTP) to enable a secure communication between two parties that have not exchanged their keys? Please draw the schematic and explain the way that this method works.

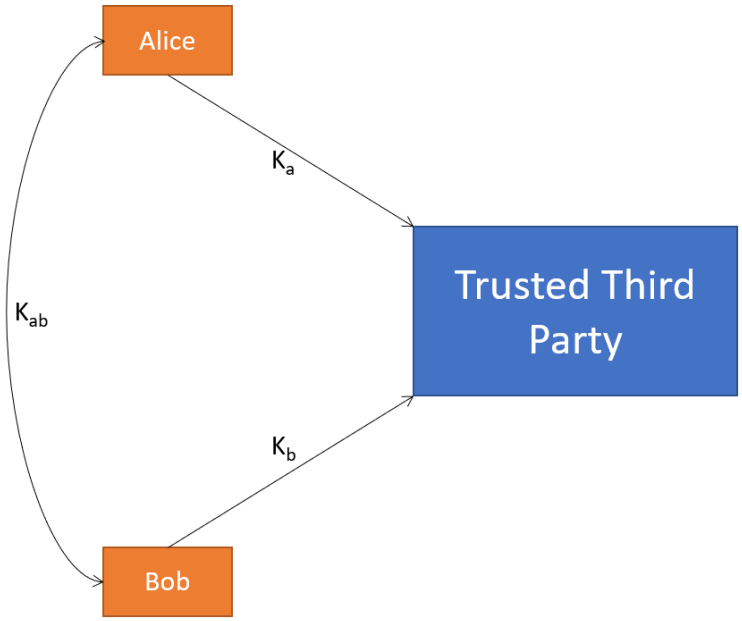

Figure 4: Schematic drawing of trusted third party.

Trusted third party takes the keys of individuals and when notified that two users want to communicate, generates a random key K_{ab} and encrypts and sends it to the users after encrypting it with their personal keys. Now the two users have a shared key and can communicate themselves.

3. What are the drawbacks of using TTP in the real world? (list two drawbacks)

   - TTP only secure against eavesdropping.
   - TTP insecure against replay attacks.
   - TTP is needed for all key exchanges (Kerberos), if compromised attacker has access to all keys.
   - Can be targeted by denial of service (DOS) attack to stop new communications.

4. What is the runtime of each of the following participants in Merkle puzzle?
   Alice: $O(n)$
   Bob: $O(n)$
   Eavesdropper: $O(n^2)$

5. Draw the schematic view and explain a scenario in which Alice and Bob exchange the keys using Diffie-Hellman protocol.

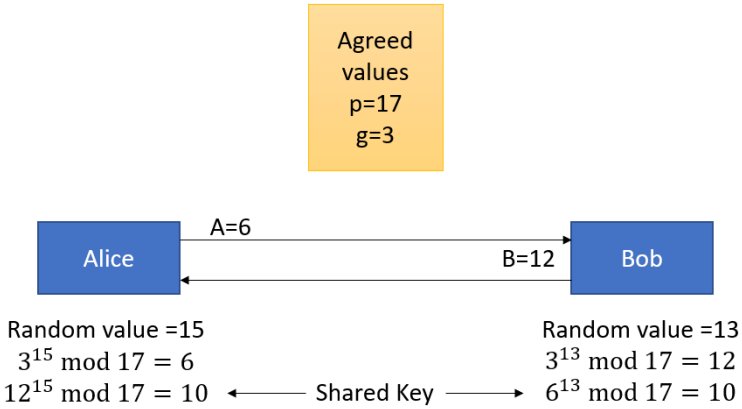

Figure 5: Schematic view of Diffie-Hellman protocol.

Bob and Alice agree publicly on a prime number p and an integer $g \in \{1, \ldots, p\}$ Alice chooses a random value $a \in \{1, \ldots, p-1\}$ and calculates $g^a \bmod p = A$ and sends this to Bob. Bob also picks a random value $b \in \{1, \ldots, p-1\}$ and calculates $g^b \bmod p = B$ and sends this to Alice. Now Alice would calculate $B^a \bmod p$ to get the shared key. Bob would calculate $A^b \bmod p$ to get the shared key.

The final calculations are the same because:

$$B^a \bmod p = g^{b^a} \bmod p = g^{ba} \bmod p$$
$$A^b \bmod p = g^{a^b} \bmod p = g^{ab} \bmod p$$

which are equivalent.