CSIT 495/595 - Introduction to Cryptography (Fall 2015)
Montclair State University
Midterm-1 Solutions

Problem 1: (15 pts)

(a). The good security guarantee is that it should be *Impossible for the attacker to know any information about the plaintext other than what he has already known*

(b). In the known-plaintext attack, the attacker is able to learn one or more plaintext/ciphertext pairs generated using some key k (of course, k is unknown to the attacker). The goal of the attacker is to deduce plaintext corresponding to some other ciphertext generated using the same key k. On the other hand, in the chosen-plaintext attack, the attacker can obtain ciphertexts corresponding to plaintexts of his/her choice. The latter attack is considered to be more powerful, so B is considered to be more secure than A.

Problem 2: (20 pts)

(a). Counter mode should be used as it provides better security as well as parallel capability for encryption and decryption. Although ECB mode provides parallel computation, it is important to note that it does not ensure ciphertext indistinguishability property (i.e., similar patterns will be preserved in the ciphertexts).

(b). In CBC mode, two blocks will get corrupted (namely blocks 50 and 51). However, in the counter mode only block 50 will be corrupted.

Problem 3: (20 pts)

(a). The main goal of authenticated encryption is to provide both data confidentiality and integrity. The three natural constructions are: (i) Encrypt-and-authenticate, (ii) Authenticate-then-encrypt, and (iii) Encrypt-then-authenticate. The third approach provides stronger security compared to the other two approaches.

(b). Re-ordering and replay attacks cannot be prevented under the given system. However, reflection attack can be prevented since Alice and Bob use different keys to explicitly address the issue of directionality.

Problem 4: (20 pts)

(a). A hash function h is said to be collision resistant if it is hard for the attacker to find two different messages m_0 and m_1 such that $h(m_1) = h(m_2)$.

(b). The following hash functions exhibit collision resistant property:

- $H'(m) = H(m) \| H(0)$
- $H'(m) = H(H(m))$

(c). The given MAC scheme does not satisfy the existential non-forgery property. For example, given a message m and its tag $t = S(k, m) = H(k||m)$, the attacker can produce a new tag $H(k||m||PB||w)$ which is a valid tag for any message w, where PB is the padding block.