CS 5158/6058 Data Security and Privacy, Spring 2018
Homework 3

Instructor: Dr. Boyang Wang

Due Date: 02/27/2018 (Tuesday), 11:59pm.
Format: Please submit a pdf of your homework in Blackboard.
Total Points: 6 points

Problem 1 (C5158 only, 1 point). Explain the difference among ciphertext-only attacks, know-plaintext attacks, and chosen-plaintext attacks.

Problem 1 (CS6058 only, 1 point). Describe the details of the security game for Chosen-Plaintext Attacks (CPA), and formally explain what is CPA-security.

Problem 2 (1 point). Describe what is a function family and what is a keyed function. Explain what is a Pseudo Random Function.

Problem 3 (1 point). Assume we have a PRG $G : \{0,1\}^n \to \{0,1\}^{2n}$, and given $n = 2$, we define this PRG as follows:

x	00	01	10	11
G(x)	1001	0011	1101	0111

If we use GGM method to build a PRF $F : \{0,1\}^m \to \{0,1\}^n$ based on this PRG G, where the input of this PRF is $x_1x_2x_3x_4x_5 = 01101$ and key $k = 01$, then what is the output of $F_k(x_1x_2x_3x_4x_5) =??$.

Problem 4 (1 point). Given a message $m = 1001111100$ and a key $k = 01$, if initialization vector $IV = 10$ and each block has 2 bits,

- what is the ciphertext of this message if we encrypt it with ECB mode?
- what is the ciphertext of this message if we encrypt it with CBC mode?

The PRF/PRP used in this block cipher is described as below.

x	00	01	10	11
$k = 00, F_k(x)$	10	00	11	01
$k = 01, F_k(x)$	00	11	01	10
$k = 10, F_k(x)$	11	01	10	00
$k = 11, F_k(x)$	01	10	00	11

Problem 5 (1 point). Given a ciphertext $c = (IV, 100111110011)$ and a key $k = 10$, if initialization vector $IV = 100$ and each block has 3 bits,

- what is the message of this ciphertext if we decrypt it with CBC mode?

– what is the message of this ciphertext if we decrypt it with OFB mode?

The PRF/PRP used in this block cipher is described as below.

x	000	001	010	011	100	101	110	111
$k = 00, F_k(x)$	100	010	011	101	111	000	001	110
$k = 01, F_k(x)$	010	011	101	111	000	001	110	100
$k = 10, F_k(x)$	101	111	000	001	110	100	010	011
$k = 11, F_k(x)$	111	101	000	001	100	110	011	010

Problem 6 (1 point). Given a message $m = 101110$, a key $k_1 = 10$ for encryption and a key $k_2 = 00$ for message authentication, assume each block has 3 bits and a random initialization vector $IV = 101$,

– compute a ciphertext and its tag using the Encrypt-then-Authenticate approach
– also explain why other approaches, such as Encrypt-and-Authenticate and Authenticate-then-Encrypt, are not suitable to protect both data privacy and message authentication.

The encryption algorithm uses CBC mode and the Mac generation algorithm also uses CBC mode. When we compute a tag for a ciphertext, we assume that the initialization vector IV is a part of a ciphertext. The PRF/PRP used in this block cipher is described as below.

x	000	001	010	011	100	101	110	111
$k = 00, F_k(x)$	100	010	011	101	111	000	001	110
$k = 01, F_k(x)$	010	011	101	111	000	001	110	100
$k = 10, F_k(x)$	101	111	000	001	110	100	010	011
$k = 11, F_k(x)$	111	101	000	001	100	110	011	010