Sean Evans
CS 6058
Data / Security and Privacy
Spring 2018
Homework 3

Problem 1

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

The security game for Chosen-Plaintext Attacks (CPA) proceeds as follows:

1. A key $k \leftarrow \text{KeyGen}(1^n)$ is generated
2. Adversary A has access to encryption oracle $\text{Enc}_k(\cdot)$, and outputs two messages m_0, m_1 with $|m_0|=|m_1|$
3. Challenger flips a fair coin $b \in \{0,1\}$, computes $c_b \leftarrow \text{Enc}_k(m_b)$, and returns c_b
4. Adversary A continues to have access to encryption oracle $\text{Enc}_k(\cdot)$
5. Adversary A guesses a bit b'
6. Outputs 1 if $b' = b$, otherwise 0; A wins if it is 1

Chosen Plaintext Attack (CPA) security is achieved for a symmetric-key encryption scheme Π if for all Probabilistic Polynomial Time (PPT) adversaries A it is indistinguishable under chosen-plaintext attacks with a negligible function such that:

$$\Pr[\text{PrivK}^{\text{cpa}}_{A,\Pi}(n) = 1] <= 1 / 2 + \text{negl}(n)$$

Evans

Problem 2

Describe what is a function family and what is a keyed function. Explain what is a Pseudo Random Function.

Function families are groupings of functions that have similar properties. A few examples of function families include polynomial, linear, exponential, rational, trigonometric, and logarithmic.

A keyed function F maps from $D = \{0,1\}^m \rightarrow R = \{0, 1\}^n$:

- First input is known as the key k
- k is chosen uniformly from K
  - $F_k(x) = F(k,x) = y$
- F is efficient (polynomial time)
- Given a key k, F_k is deterministic

F is a Pseudo Random Function (PRF) if F_k is indistinguishable from f

- k is chosen uniformly from K
- f is chosen uniformly from Func(m, n)

Pseudo Random Functions can be defined in the following way:

Let $F = \{0,1\}^l \times \{0,1\}^m \rightarrow \{0,1\}^n$ be an efficient keyed function. F is a PRF if for all Probabilistic Polynomial Time (PPT) adversaries A there is a negligible function such that

$$|\Pr[A^{Fk(\cdot)}(1^l) = 1] - \Pr[A^{f(\cdot)}(1^l) = 1]| <= \text{negl}(l)$$

Problem 3

Assume we have a PRG G: $\{0,1\}^n \rightarrow \{0,1\}^{2n}$, 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: $\{0,1\}^m \rightarrow \{0,1\}^n$ 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 $F_k(x_1x_2x_3x_4x_5)$ = ??.

$x_1 = 0$
$x_2 = 1$
$x_3 = 1$
$x_4 = 0$
$x_5 = 1$

$F_k(x_1x_2x_3x_4x_5) = G_{x5}(G_{x4}(G_{x3}(G_{x2}(G_{x1}(k))))) = \ldots$

$F_{01}(01101) = G_1(G_0(G_1(G_1(G_0(01))))) = ...$

$G(01) = 0011 \rightarrow G_0(01) = 00$

$G_1(G_0(G_1(G_1(G_0(01))))) = G_1(G_0(G_1(G_1(00)))) = \ldots$

$G(00) = 1001 \rightarrow G_1(00) = 01$

$G_1(G_0(G_1(G_1(00)))) = G_1(G_0(G_1(01))) = \ldots$

$G(01) = 0011 \rightarrow G_1(01) = 11$

$G_1(G_0(G_1(01))) = G_1(G_0(11)) = \ldots$

$G(11) = 0111 \rightarrow G_0(11) = 01$

$G_1(G_0(11)) = G_1(01) = \ldots$

$G(01) = 0011 \rightarrow G_1(01) = 11$

$\underline{F_{01}(01101) = 11}$

Problem 4

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

$m_1 = 10$
$m_2 = 01$
$m_3 = 11$
$m_4 = 11$
$m_5 = 00$

$c_x = F_k(m_x)$
$c_1 = F_{01}(10) = 01$
$c_2 = F_{01}(01) = 11$
$c_3 = F_{01}(11) = 10$
$c_4 = F_{01}(11) = 10$
$c_5 = F_{01}(00) = 00$

$\underline{c_{ecb}} = 01\ 11\ 10\ 10\ 00$

$c_x = F_k(m_x \oplus c_{x-1})$
$c_0 = IV = 10$
$c_1 = F_{01}(m_1 \oplus c_0) = F_{01}(10 \oplus 10) = F_{01}(00) = 00$
$c_2 = F_{01}(m_2 \oplus c_1) = F_{01}(01 \oplus 00) = F_{01}(01) = 11$
$c_3 = F_{01}(m_3 \oplus c_2) = F_{01}(11 \oplus 11) = F_{01}(00) = 00$
$c_4 = F_{01}(m_4 \oplus c_3) = F_{01}(11 \oplus 00) = F_{01}(11) = 10$
$c_5 = F_{01}(m_5 \oplus c_4) = F_{01}(00 \oplus 10) = F_{01}(10) = 01$

$\underline{c_{cbc}} = 10\ 00\ 11\ 00\ 10\ 01$

Problem 5

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

c_0 = IV = 100
c_1 = 100
c_2 = 111
c_3 = 110
c_4 = 011

$m_i = F_k^{-1}(c_i) \oplus c_{i-1}$
$m_1 = F_{10}(c_1) \oplus c_0 = F_{10}(100) \oplus 100 = 110 \oplus 100 = 010$
$m_2 = F_{10}(c_2) \oplus c_1 = F_{10}(111) \oplus 100 = 011 \oplus 100 = 111$
$m_3 = F_{10}(c_3) \oplus c_2 = F_{10}(110) \oplus 111 = 010 \oplus 111 = 101$
$m_4 = F_{10}(c_4) \oplus c_3 = F_{10}(011) \oplus 110 = 001 \oplus 110 = 111$

$\underline{m_{cbc} = 010\ 111\ 101\ 111}$

$x_i = F_k^{-1}(x_{i-1})$
$x_0 = IV = 100$
$x_1 = F_{10}(x_0) = F_{10}(100) = 110$
$x_2 = F_{10}(x_1) = F_{10}(110) = 010$
$x_3 = F_{10}(x_2) = F_{10}(010) = 000$
$x_4 = F_{10}(x_3) = F_{10}(000) = 101$

$m_i = c_i \oplus x_i$
$m_1 = c_1 \oplus x_1 = 100 \oplus 110 = 010$
$m_2 = c_2 \oplus x_2 = 111 \oplus 010 = 101$
$m_3 = c_3 \oplus x_3 = 110 \oplus 000 = 110$
$m_4 = c_4 \oplus x_4 = 011 \oplus 101 = 110$

$\underline{m_{ofb} = 010\ 101\ 110\ 110}$

Problem 6

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

$m_1 = 101$
$m_2 = 110$

$c_x = F_k(m_x \oplus c_{x-1})$
$c_0 = IV = 101$
$c_1 = F_{10}(m_1 \oplus c_0) = F_{10}(101 \oplus 101) = F_{10}(000) = 101$
$c_2 = F_{10}(m_2 \oplus c_1) = F_{10}(110 \oplus 101) = F_{10}(011) = 001$

$\underline{c_{cbc}}$ = 101 101 001

$t = F_{00}(F_{00}(F_{00}(c_0) \oplus c_1) \oplus c_2) =$
$F_{00}(F_{00}(F_{00}(101) \oplus 101) \oplus 001) =$
$F_{00}(F_{00}(000 \oplus 101) \oplus 001) =$
$F_{00}(F_{00}(101) \oplus 001) =$
$F_{00}(000 \oplus 001) =$
$F_{00}(001) =$

$\underline{t}$ = 010

Approaches such as Encrypt-and-Authenticate and Authenticate-then-Encrypt are not suitable to protect privacy and message authentication because they are not probabilistic, and therefore are not secure against Chosen Plaintext Attack (CPA). This is because the message authentication code (MAC) in both of these schemes are based solely on the plaintext and therefore the MAC is deterministic. While in the Encrypt-then-Authenticate approach, the probabilistic output from the encryption is used as input into the hash, thus making the MAC probabilistic and therefore CPA secure.