Hardware-Oriented Security and Trust
ECE 4156 HST / ECE 6156 HST
Spring 2024
Assoc. Prof. Vincent John Mooney III
Georgia Institute of Technology
Homework 2, 30 pts. (ECE 4156) 40 pts. (ECE 6156)
Due Friday January 19 prior to 11:55pm

1) (10 pts.) In the Media Gallery on Canvas, listen to the second half (approximately from the 29 minute point in the lecture to the end at 58 minutes) of lecture "03IntroSHA2." There is no need to notify Professor Mooney that you have done so **unless** you have problems. Canvas provides information regarding which GT usernames have accessed / listened to lectures, so there is no need to turn anything in if you have been successful.

Watch the video uploaded on Canvas.

2) (10 pts.) Consider the following encryption scheme. The message space is $M = \{0, \dots, 4\}$. Algorithm Gen chooses a uniform key from the key space $\{0, \dots, 5\}$. $\mathrm{Enc}_k(m)$ returns result $[k + m \ mod \ 5]$, and $\mathrm{Dec}_k(c)$ returns $[c - k \ mod \ 5]$. Does this scheme fit the definition of "perfect" secrecy, i.e., either Definition 2.3 or Definition 2.5?

(NOTE: this is part a of problem 2.6 on page 38 of Katz and Lindell.)

Solution

DEFINITION 2.3 *Encryption scheme* π = (Gen, Enc, Dec) *with message space* M *is* **perfectly secret** *if for every probability distribution over* M, *every message* $m \in M$, *and every ciphertext* $c \in C$ *for which* $\Pr[C = c] > 0$:

$$\Pr[M = m | c \in C] = \Pr[M = m].$$

Given Message Space M = {0, … ,4}
Key Space K = {0, … ,5}

From the key space and message space, a table of every ciphertext from all combinations of plaintext and keys is shown below. The values in the table cells are the encrypted ciphertext for all pairs of messages and keys.

M	K =>	0	1	2	3	4	5
0		0	1	2	3	4	0
1		1	2	3	4	0	1
2		2	3	4	0	1	2
3		3	4	0	1	2	3
4		4	0	1	2	3	4

$$\Pr[M = 1] = \frac{1}{5}\left[1\; is\; \frac{1}{5}\; of\; set\; [1,5]\right]$$

$$\Pr[C = 1] = \frac{6}{30}\; [Total\; Number\; of\; Occurences]$$

From Baye’s Theorem

THEOREM A.8 (Bayes’ Theorem) *If* $\Pr[E_2] \neq 0$ *then*

$$\Pr[E_1 | E_2] = \frac{\Pr[E_1|E_2] \cdot \Pr[E_1]}{\Pr[E_2]}.$$

Therefore

$$\Pr\left[\frac{[M = 1]}{[C = 1]}\right] = \frac{\Pr[M = 1] \times \Pr\left[\frac{[C = 1]}{[M = 1]}\right]}{\Pr[C = 1]}$$

$$= \frac{\frac{1}{5} \times \Pr\left[\frac{[C = 1]}{[M = 1]}\right]}{\frac{1}{5}}$$

$$\Pr\left[\frac{[C = 1]}{[M = 1]}\right] = \frac{2}{6}[\,1\; is\; repeated\; twice\; when\; M = 1]$$

$$= \frac{1}{3}$$

$$As\; per\; Def\; 2.3\;\; \Pr[M = 1] \;=\; \Pr\big[[M = m]||[\,C = c]||\big]$$

$$But\; the\; value\; obtained\; is\; \frac{1}{5} \neq \frac{1}{3}$$

Hence, the given scheme does not fit the definition of perfect secrecy.

3) (10 pts.) When using a one-time pad with k = 0^ℓ, we have Enc$_\mathrm{k}(m)$ = $k \oplus m$ = m and the message is sent in the clear! It has therefore been suggested to modify the one-time pad by only encrypting with $k \neq 0^\ell$ (i.e., have Gen choose k uniformly from the set of *nonzero* keys of length ℓ). Is this modified scheme perfectly secret, i.e., does this scheme fit the definition of either Definition 2.3 or Definition 2.5? Explain.

(NOTE: this is problem 2.7 on page 38 of Katz and Lindell.)

Solution

DEFINITION 2.3 *Encryption scheme* π = (Gen, Enc, Dec) *with message space* M *is* **perfectly secret** *if for every probability distribution over* M*, every message* $m \in M$*, and every ciphertext* $c \in C$ *for which* $\Pr[C = c] > 0$ **:**

$$\Pr[M = m | c \in C] = \Pr[M = m].$$

From the given definition, all the scheme is perfectly true for all cases except for the K = 0^l.
Considering K = 0^l
we find that $\Pr\left[\frac{M=0}{C=0}\right] = 0$
where the definition has been given that $\Pr[M = 0] > 0$

$$\therefore \Pr\left[\frac{M = 0}{C = 0}\right] \neq \Pr[M = 0]$$

Hence this scheme fails for Def. 2.3 and is not perfectly secret.

∴ The modified scheme is “not perfectly secret” according to Definition 2.3 or Definition 2.5.

4) [ECE 6156 only!] (10 pts.) Consider the following encryption scheme. The message space is M = $\{m \in \{0,1\}^{\ell}$ | the last bit of m is 0$\}$. (Note that | means "such that." In other words, every message m has ℓ bits with the last bit always equal to zero.) Algorithm Gen chooses a uniform key from the key space $\{0,1\}^{\ell-1}$. Enc$_{\mathrm{K}}(m)$ returns a ciphertext result of $m \oplus (k \parallel 0)$, and Dec$_{\mathrm{K}}(c)$ returns $c \oplus (k \parallel 0)$. Does this scheme fit the definition of "perfect" secrecy, i.e., either Definition 2.3 or Definition 2.5?

(NOTE1: $k \parallel 0$ denotes concatenation of k followed by 0. For example, if k = 0110 then $k \parallel 0$ = 01100.)

(NOTE2: this is part b of problem 2.6 on page 38 of Katz and Lindell.)

Solution

Given that the last bit is always 0, the size of M is reduced

M size = 2^{l-1}

K size is also specified as l-1 bits; K size = 2^{l-1}

$$Enc_k(m) = m \oplus (k \parallel 0)$$

Here the last digit of the message is always zero, i.e., 0 is appended to the original message. The result is that the size of M decreases. The further result is that the sizes of K and M are the same so that all the conditions given by Def 2.3 should hold true.

$$\Pr\left[\frac{M=m}{C=c}\right] = \Pr[M=m]$$

Using Baye's Theorem

THEOREM A.8 (Bayes' Theorem) *If* $\Pr[E_2] \neq 0$ *then*

$$\Pr[E_1 | E_2] = \frac{\Pr[E_1|E_2] \cdot \Pr[E_1]}{\Pr[E_2]}.$$

Therefore

$$\Pr\left[\frac{M=m}{C=c}\right] = \frac{\Pr[M=m] \times \Pr\left[\frac{C=c}{M=m}\right]}{\Pr[C=c]}$$

It is known that $\Pr\left[\frac{C=c}{M=m}\right] = \Pr[Enc[m]] = (2^{l-1})$

It is also known that $\Pr[C=c] = (2^{l-1})$

$$= \Pr[M=m] \times \frac{(2^{l-1})}{(2^{l-1})}$$

$$= \Pr[M=m]$$

$$\therefore \Pr\left[\frac{M=m}{C=c}\right] = \Pr[M=m]$$

Therefore, the given scheme fits the definition of "perfect Secrecy."