Brian Yee - 00993104
Introduction to Cryptography CPSC 418 Fall 2016
Department of Computer Science
University of Calgary

October 21, 2016

HOME WORK #2

Problem	Marks
1	
2	
3	
4	
5	
6	
7	
Total	

Problem 1. Conditional entropy

1.a)

$$H(M|C) = \sum_{c \in C} p(C) \sum_{m \in M} p(M|C) log_2(\frac{1}{p(M|C)})$$

$H(M|C) = \sum p(C) \sum p(M|C) log_2(\frac{1}{p(M|C)})$
$= \frac{1}{4}(\frac{1}{2} log_2(2) + \frac{1}{2} log_2(2)) + \frac{1}{4}(\frac{1}{2} log_2(2) + \frac{1}{2} log_2(2)) + \frac{1}{4}(\frac{1}{2} log_2(2) + \frac{1}{2} log_2(2)) + \frac{1}{4}(\frac{1}{2} log_2(2) + \frac{1}{2} log_2(2))$

1.b)
Since the cryptosystem provides perfect secrecy, $p(x|y) = p(x)$.
$\sum p(M) log_2(\frac{1}{p(M)})$
$= \frac{1}{|M|} log_2(\frac{1}{p(M)}) + \frac{1}{|M|} log_2(\frac{1}{p(M)}) + ... + \frac{1}{|M|} log_2(\frac{1}{p(M)})$ ($|M|$ total terms)
$= |M| * \frac{1}{|M|} log_2(\frac{1}{p(M)})$
$= log_2(\frac{1}{p(M)})$

$H(M|C) = \sum p(C) \sum p(M|C) log_2(\frac{1}{p(M|C)})$
$= \sum p(C) \sum p(M) log_2(\frac{1}{p(M)})$
$= \sum p(C) log_2(\frac{1}{p(M)})$

$p(C) = \frac{p(C|M)p(M)}{p(M|C)}$
$p(C) = \frac{p(C|M)p(M)}{p(M)}$
$p(C) = p(C|M)$
...
$= \sum p(M) log_2(\frac{1}{p(M)})$
$= H(M)$

1.c)
No, since $p(M|C) = \frac{1}{2} \neq \frac{1}{4} = p(M)$.

$\longrightarrow$ $\mathcal{A}$nswer

Problem 2. Binary polynomial arithmetic

2.a.i)
x^3
$x^3 + 1$
$x^3 + x$
$x^3 + x + 1$
$x^3 + x^2$
$x^3 + x^2 + 1$
$x^3 + x^2 + x$
$x^3 + x^2 + x + 1$

2.a.ii)
$x^3 = x * x * x$
$x^3 + 1 = (x + 1)(x^2 - x + 1)$
$x^3 + x = x(x^2 + x)$
$x^3 + x + 1 =$ irreducible
$x^3 + x^2 = x^2(x + 1)$
$x^3 + x^2 + 1 =$ irreducible
$x^3 + x^2 + x = x(x^2 + x + 1)$
$x^3 + x^2 + x + 1 = (x + 1)(x^2 + 1)$

2.a.iii)

$\longrightarrow$ $\mathcal{A}$nswer

Problem 3. Arithmetic with the constant polynomial of MixColumns in AES

1.a)

$\longrightarrow \mathcal{A}$nswer

Submitted by Brian Yee - 00993104 on October 21, 2016.