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

October 10, 2016

HOME WORK #2

Problem	Marks
1	
2	
3	
4	
5	
6	
7	
Total	

Problem 1. Conditional entropy

Problem 2. Binary polynomial arithmetic $\longrightarrow \mathcal{A} \text{nswer}$ Problem 3. Arithmetic with the constant polynomial of MixColumns in AES $\longrightarrow \mathcal{A} \text{nswer}$

Submitted by Brian Yee - 00993104 on October 10, 2016.