

Spring 2023 - ICSI 526

Homework 4

Written by Jacob Clouse

April 30, 2023

Contents

1	Question 1	1
1.1	Implement hash function A ($n = p \times q$)	1
1.2	Implement hash function B ($h_2(m) = M_1 \oplus M_2 \dots \oplus M_n$)	1
2	Question 2	1
2.1	Design and implement a PRNG using AES (OFB mode)	1
2.2	Calculate the Fraction of One Bits	1

1 Question 1

1.1 Implement hash function A ($n = p \times q$)

Implement A...

1.2 Implement hash function B ($h_2(m) = M_1 \oplus M_2 \dots \oplus M_n$)

Implement B...

2 Question 2

2.1 Design and implement a PRNG using AES (OFB mode)

Design Algo...

2.2 Calculate the Fraction of One Bits

Calculate FOOB...