Spring 2023 - ICSI 526
Homework 4

Written by Jacob Clouse

April 30, 2023

Contents

1 Question 1

1.1 Implement hash function A (n = p x q)

Implement A...

1.2 Implement hash function B (h2(m) = M1 ⊕ M2 ... ⊕ Mn.)

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...