Cryptographic Secret Sharing

Girls Talk Math

Introduction

In this problem set, you will learn about ...

One last note about reading mathematical texts: it is very normal when reading math to read a passage or even a single sentence several times before understanding it properly. Also, never trust the author! Check every claim and calculation (time permitting). Take your time and never give up. Let's talk math!

Contents

1 Probability and Randomness

1.1 Introduction

1.2 Randomness in Cryptography

Define *information-theoretic security*.

1.3 Sharing Secrets

Secret sharing is a way to...

2 A simple secret sharing

2.1 Binary Arithmetic

The exclusive-OR (XOR) operation is denoted by the symbol $\oplus$ and defined by the following truth table:

a	b	$a \oplus b$
0	0	0
0	1	1
1	0	1
1	1	0

2.2 Sharing Secrets using XOR

3 Shamir's Secret Sharing

3.1 Polynomials

y-intercept, zeroes

3.1.1 Uniqueness

How many points uniquely define a polynomial

Exercise 3.1

3.2 Sharing Secrets Using Polynomials

Don't introduce finite fields but maybe make a note that this should be done over finite fields.