Investigating whether the inputs of a Multiplicative Congruential Random Number Generator can be determined using a sufficient amount of outputs

Yohwllo

Febuary 14th 2024

Contents

1 Introduction

Ever since I was a young child I've wanted to break, and reverse engineer computers, and everything related to them. Whether it be encryption, or the hardware I've wanted to break it down to its smallest components, and figure out how to reverse it on a dime. In terms of encryption, a lot of badly built programs used a random number generator called a Linear Congruential Generator. This type of number generator is extremely sensitive to input, and does not create truely random numbers, yet they are still often used in crypographic implementations due to naivite. This causes a lot of encrypted information to be broken, and what not. For this reason I will be investigating a better, and quicker method to determing the input parameters to an LCG.

myBib

2 Background

2.1 Linear Congruential Generators

asdsad [**guglani2008transient**]