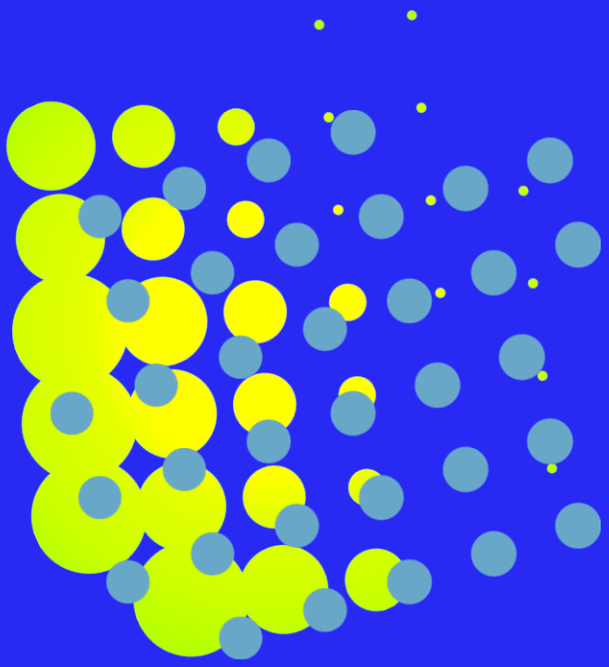

d3cryptOr

Cryptanalysis of a class of ciphers based on Frequency Analysis Technical Report

Iman Hosseini - Karthik Venkatesh

Contents

1 INTRODUCTION

This project is done by Iman Hosseini and Karthik Venkatesh.

2 INTUITION

A motivating example.

3 QUANTITIVE ANALYSIS

4 IMPLEMENTATION: D3CRYPT0R

5 PERFORMANCE ANALYSIS

6 PLANNING

We started the project early, aiming to produce a project of good quality. At the github repository of the project the exact details of how the project proceeded can be seen. As of 17th September, we had an implementation of the encryption and decryption algorithm in Python, plus the main idea for checking whether a ciphertext can be generated from a given plaintext, and the basics of our c++ code. The initial version of this report was also ready (with logo design etc.). The report was done with LaTeXusing overleaf.

It was decided to implement and prototype ideas in python, which requires less development time, and then implement the final decryptor in C++ where it can be optimized to be blazing fast. This also would make possible, an analysis of the speedup provided by C++.

7 RIGOROUS TREATMENT

8 SURVEY OF PERMUTATION CIPHERS

TBD

9 SURVEY OF CRYPTANALYSIS OF PERMUTATION CIPHERS

TBD