

CS 163 Coin Flipping Lab

Fall 2019

September 24, 2019

1 Introduction

In this lab, you are going to generate cryptographic keys by hand. A cryptographic key is a sequence of bits that is used to encrypt information.

Example: WiFi WPA Encryption Most WiFi networks use a technique called WPA to encrypt network traffic. If you don't have the encryption key, you cannot decode the data that goes through the network. This is important for wireless networks because anybody within a few feet of your computer can listen to your packets, and you don't want them to be able to decode everything you're sending (email, web traffic, etc). WiFi network encryption keys are generated from passwords. You type in the password on your laptop, and your computer uses a special function called a hashing function to convert the password text into a 64-bit key. That key is then used to encrypt and decrypt network traffic, so even if someone eavesdrops on your network packets, the data they record will be gibberish.

In this lab, we will be directly generating 5-bit network keys by flipping a coin. We will say that when the coin lands on Heads, that corresponds to a 1 bit. When it lands Tails, that corresponds to a 0 bit.

How many possible keys can we generate using 5 bits?

Instructions for Generating Keys Each row in the table below corresponds to one key. For each row, flip a coin eight times and record a 1 or a 0 in the boxes labelled bits. If the coin lands on Heads, put a 1 in the box. If it lands tails, put a 0. Leave the Decimal column blank until you've filled out all the bits.

| | Bits | | | | | Decimal |
|----------------|------|---|---|---|---|---------|
| Example | 1 | 0 | 1 | 1 | 0 | 22 |
| Key 1 | | | | | | |
| Key 2 | | | | | | |
| Key 3 | | | | | | |
| Key 4 | | | | | | |
| Key 5 | | | | | | |
| Key 6 | | | | | | |
| Key 7 | | | | | | |
| Key 8 | | | | | | |
| Key 9 | | | | | | |
| Key 10 | | | | | | |
| Key 11 | | | | | | |
| Key 12 | | | | | | |
| Key 13 | | | | | | |
| Key 14 | | | | | | |
| Key 15 | | | | | | |

Use a binary-to-decimal converter such as:
<https://www.rapidtables.com/convert/number/binary-to-decimal.html>