Number of bits to be flipped to get random bitstream: 3

|  |
| --- |
| **Graph of the results:** |

Graph for all key sizes (Combined):

Figure 1 Combined graph for all sizes of key streams. Please look at individual graphs for the actual curve.

Graphs for individual key sizes:

X-axis: the number of bits flipped

Y-axis: Randomness

Figure 2 Size: 8192 bits (1024 Bytes)

Figure 3 Size: 1024 bits (128 Bytes)

Figure 4 Size: 256 bits (32 Bytes)

Figure 5 Size: 64 bits (8 Bytes)

Figure 6 Size: 32 bits (4 Bytes)

Figure 7 Size: 2 bits (16 Bytes)

|  |
| --- |
| **Part 2:** |

**Observations:**

1. Randomness increases with the increase in number of bits i.e the randomness becomes closer to 0 when number of bits in key are increased and vulnerability decreases.
2. If we use 256 RC4 key for 1024-bit key stream generation, it works way better as compared to 8 bit RC4 key for the same purpose.
3. On an average 9-14 bits need to be flipped before the differential bitstream looks random. This depends on the key size we are using.
4. For RC4 to work securely, first kN Bytes must be discarded. Where N = 256 and k>=3 which implies that atleast the first 768 Bytes need to be discarded.
5. For a vendor who wants to send 50 Bytes of message, he should generate a key of length atleast 818Bytes (768+50 Bytes).
6. Out of these 818 Bytes, the first 768 should be discarded and the next 50 can be used for encryption and decryption.
7. This is done to protect the cipher text from Fluhrer, Mantin and Shamir attacks which make use of the fact that first few bytes of generated key are not random.