Random Bit Tests

Although it's impossible to prove if a stream of bits is random, we can check to see if a stream of bits satisfies some standard qualities of a theoretically random stream of bits. We would like our key bitstreams to be random so that Eve can't determine patterns in the key bitstream.

Here is an example of a set of test from the FIPS 140-1 poker set:

For a stream of 20,000 random bits:

1) The number of 0s must be in between 9654 and 10346

2) The distribution of the four bit segments (0 - 15) should be roughly equal. For the standard, let n_i represent the number of occurrence of i when we divide the bit stream up into 5000 blocks of 4 bits. Then we calculate a value X as follows:

$$X = \frac{16}{5000}\sum_{i=0}^{15} {n_i}^2 - 5000$$

This test passes if $1.03 < X < 57.4$.

3) A runs test sees how many runs of the same bit consecutively appear. Here are the requirements for our specific test:

Length of Run	Number of occurrences
1	2267-2733
2	1079-1421
3	502-748
4	223-402
5	90-223
6+	90-223