|  |  |  |  |
| --- | --- | --- | --- |
| **Party A** | | **Party B** | |
| t = 0 |  | t = 0 |  |
| t = 750 \_ 1750 ms | tone | t = 0\_ 3000 ms | record |
| t = 2500 \_ 5500 ms | record | t = 3500 \_ 4500 ms | tone |

**Key Generation Rate (KGR):**

It quantifies the number of key bits generated in each second, which can be given where *Nk* is the number of keys and *Tk* is the time taken.



* Tk = (5500 \* 10-3) sec + avg\_T\_quantize\_reconcile\_amplify\_privacy
* avg\_T\_quantize\_reconcile\_amplify\_privacy = 0.3 sec
* KGR = (final length before privacy amplification / Tk) = 23.27 bit/sec

|  |
| --- |
| **Output example** |
| \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* [ KEY\_AB ] \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*   \_\_\_\_\_\_\_ 1. QUANTIZATION \_\_\_\_\_\_\_  Responder string length before reconciliation: 234 Initiator string length before reconciliation: 234 Key stings are not equal and they need reconciliation (cascade)  \_\_\_\_\_\_\_ 2. CASCADE \_\_\_\_\_\_\_  Mismatches number = 89 bit error rate (probability) Pe: 0.3803418803418803 basic block size: 4   ---Cascade Statistics--- There were 89 errors found and corrected: There obs Error Rate: 0.3803418803418803 The total number of disclosed bits is 115 They are equal now Initial\_Shared\_Key --- of length 234 is:  [0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]  \_\_\_\_\_\_\_ 3. PRIVACY AMPLIFICATION \_\_\_\_\_\_\_  Final\_Shared\_Key --- of length 128 is:  [1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1] Final\_Shared\_Key\_Dec\_AB = 329341657347407614360263427846181963189  \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* [ KEY\_BC ] \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*   \_\_\_\_\_\_\_ 1. QUANTIZATION \_\_\_\_\_\_\_  Responder string length before reconciliation: 219 Initiator string length before reconciliation: 219 Key stings are not equal and they need reconciliation (cascade)  \_\_\_\_\_\_\_ 2. CASCADE \_\_\_\_\_\_\_  Mismatches number = 91 bit error rate (probability) Pe: 0.4155251141552511 basic block size: 4   ---Cascade Statistics--- There were 91 errors found and corrected: There obs Error Rate: 0.4155251141552511 The total number of disclosed bits is 120 They are equal now Initial\_Shared\_Key --- of length 219 is:  [0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]  \_\_\_\_\_\_\_ 3. PRIVACY AMPLIFICATION \_\_\_\_\_\_\_  Final\_Shared\_Key --- of length 128 is:  [1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1] Final\_Shared\_Key\_Dec\_BC = 280307171578841709315472758261233912795  \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Compare Keys \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  Final\_Shared\_Key\_Dec\_AB = 329341657347407614360263427846181963189 Final\_Shared\_Key\_Dec\_BC = 280307171578841709315472758261233912795  **Different Keys** |

Randomness tests:

|  |
| --- |
| **p-value:** The probability that the chosen test statistic will assume values that are equal to or worse than the observed test statistic value. The *P-value* is frequently called the “tail probability.” |
| **T E S T S** |
| **Frequency (Monobit) Test:**  **The purpose of this test is to determine whether the number of ones and zeros in a sequence are approximately the same as would be expected for a truly random sequence.**  Since *P-value* ≥*0.01*, accept the sequence as random. |
| **Frequency Test within a Block:**  The purpose of this test is to determine whether the frequency of ones in an M-bit block is approximately M/2, as would be expected under an assumption of randomness. For block size *M*=1, this test degenerates to test 1, the Frequency (Monobit) test.  Since P-value 0.01, accept the sequence as random. |
| **Runs Test:**  The focus of this test is the total number of runs in the sequence, where a run is an uninterrupted sequence of identical bits. A run of length *k* consists of exactly *k* identical bits and is bounded before and after with a bit of the opposite value. The purpose of the runs test is to determine whether the number of runs of ones and zeros of various lengths is as expected for a random sequence. In particular, this test determines whether the oscillation between such zeros and ones is too fast or too slow.  Since *P-value* ≥*0.01*, accept the sequence as random. |
|  |
|  |
|  |
|  |
|  |