|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| S.No. | **Methods**  **Types of Test** | **XRSA** | **ESRKGS** | **RSA** | **MRSA** |
| 1. | FIPS Monobit | 5 bits failed the test | 10 bits failed the test | 5 bits failed the test | 4 bits failed the test |
| 2. | FIPS Poker Test | 5 bits failed the test | 8 bits failed the test | 1 bit failed the test | 63 bits failed the test |
| 3. | FIPS Run Test | 2 bits failed the test | 4 bits failed the test | All bits passed the test | 1 bit failed the test |
| 4. | FIPS Long Run Test | 3 bits failed the test | 5 bits failed the test | 2 bits failed the test | 2 bit failed the test |
| 5. | Spectral Tests | 1107 Anomalies identified | 2115 anomalies identified | 515 Anomalies identified | 417 anomalies identified |
| 6. | Correlation | 1 Anomalies identified | 8 Anomalies identified | No Anomalies Identified | No Anomalies Identified |
| 7. | Compression | 1 Anomaly identified | 2 Anomalies identified | No Anomalies identified | 1 Anomaly identified |
|  | Summary | Based on the 1000 tokens sample size, the reliability of PRNG is “reasonable”.  The overall randomness quality is “excellent” | Based on the 1000 tokens sample size, the reliability of PRNG is “reasonable”.  The overall randomness quality is “excellent” | Based on the 1000 tokens sample size, the reliability of PRNG is “reasonable”.  The overall randomness quality is “excellent” | Based on the 1000 tokens sample size, the reliability of PRNG is “reasonable”.  The overall randomness quality is “excellent” |

T Table: Comparison of methods using Burp sequencer