Trivium Cipher

CS4062D Introduction to Information Security

Code files:

https://github.com/arunnats/NITC-Information-Security-S6/tree/main/trivium

Raw output:

https://raw.githubusercontent.com/arunnats/NITC-Information-Security-S6/refs/heads/main/trivium/finalAnalysisReport.txt

Output table: I have encapsulated the raw data to the required format as the NIST output had a lot more rows than expected.

SL.No	Test name	P-value	Status
1	Frequency	0.122325	Pass
2	Block frequency	0.162606	Pass
3	Cumulative sums	0.051383	Pass
4	Runs	0.030809	Pass
5	Longest Run	0.137282	Pass
6	Rank	0.955835	Pass
7	FFT	0.779188	Pass
8	Non overlapping template	0.924076	Pass
9	Overlapping template	0.678686	Pass
10	Universal	0.798139	Pass
11	Approximate entropy	0.023545	Pass
12	Random excursions	0.739918	Pass
13	Random excursions variant	0.834308	Pass
14	Serial	0.574903	Pass
15	Linear complexity	0.759756	Pass

Inferences: The Trivium cipher output passed all 15 NIST statistical tests, with each test showing a "Pass" status and reasonable P-values. This means Trivium produces keystreams that look random and do not show obvious patterns. NIST tests work by checking if a sequence is similar to true random data using various mathematical checks. Stream ciphers like Trivium are designed to be fast and secure, but their security also depends on how they are used, such as never reusing the same key or IV. Overall, using NIST tests helps us confirm that Trivium, and similar stream ciphers, generate output suitable for cryptography.