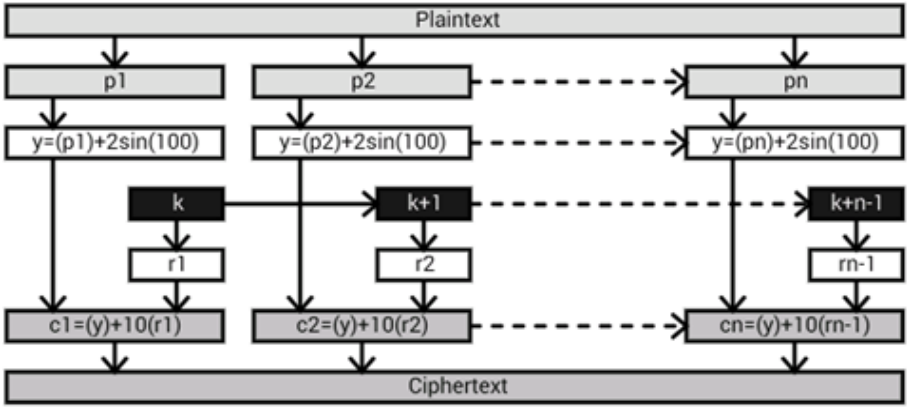
An Improved Method for PRNG-Based Text Encryption

Protecting confidentiality of data over a computer network is one of the three pillars of information security and with increasing sophistication of cyber attacks, investigating new solutions is essential to mitigate information leak.

Invention:

This invention is an improved symmetric-stream encryption method based on pseudo-random number generators (PRNG).



Encryption block diagram of the RNG based method.

Advantages:

- Immune to all known-plaintext cryptanalysis attacks and provides large plaintext and key sensitivity ranging from 40%-50%.
- Provides a secure method for communicating data with low computational requirements.
- Suitable for bandwidth-limited environments.

Market Opportunity:

The global encryption software market accounted for about USD 2.20 billion in 2015 and is expected to reach around USD 7.17 billion by 2021, growing at a CAGR of around 21.7% between 2016 and 2021.

Current status:

This system has been benchmarked using some preliminary industry standards like AES 128bit encryption.

IP Protection:

Patent application# US 15/241333 (Non provisional)
Country of Filing: United States

Route to Market:

Needs to be tested with a real chat application (or a simple chat application be built).

Next Steps:

- The current code is built using MATLAB R2014b. (known performance limitations). Encryption time and throughput can be improved further if implemented on a faster platform.
- Industry Feedback to estimate the size and fit of opportunity.
- Perform standardization: AES, CRYPTREC, NESSIE.