4-11-2011

Linear Feedback Shift Registers: Pseudo-Random Number Generators and Their Use In Cryptosystems

Michael Perez
Department of Mathematics, Boise State University

Marion Scheepers
Department of Mathematics, Boise State University

Linear Feedback Shift Registers: Pseudo-Random Number Generators and Their Use In Cryptosystems

Abstract

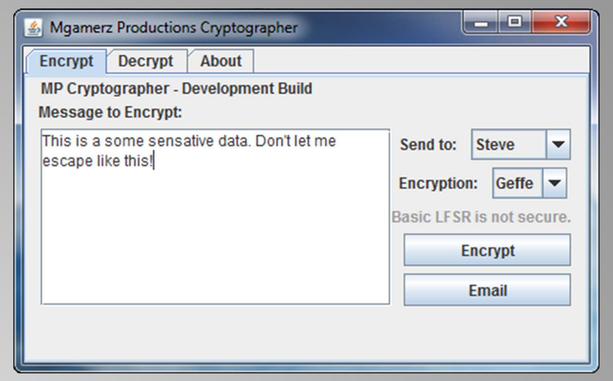
Cryptology is the study and application of encrypting and decrypting data so that only the intended recipient and senders can view data. This is important in applications such as online banking and military operations. Linear Feedback Shift Registers, or LFSRs for short, create a pseudo-random number stream that is computationally efficient. LFSRs are used (in conjunction with other methods) to encrypt items such as DVD's and many wireless signals, including digital TV and radio. Using random methods, a seed value can be created to create a strong random number stream.

Disciplines

Mathematics

Linear Feedback Shift Registers: Pseudo-Random Number Generators and Their Use In Cryptosystems

Michael Perez
Dr. Marion Scheepers



Project Background

Cryptology is the study and application of encrypting and decrypting data so that only the intended recipient and senders can view data. This is important in applications such as online banking and military operations. Linear Feedback Shift Registers, or LFSRs for short, create a pseudo-random number stream that is computationally efficient. LFSRs are used (in conjunction with other methods) to encrypt items such as DVD's and many wireless signals, including digital TV and radio. Using random methods, a seed value can be created to create a strong random number stream.

Project Objectives

Develop an email encryption program that:

- Takes input text that applies cryptographic methods to ensure third parties cannot read the message
- Generate RSA keys for a group that can be used with the cryptographer
- Send keys securely using RSA for safe decryption

Methods

The email encryption program was originally written in a beginner language called GML, as a demo. It was later ported to Java, with some functions ported to MAPLE scripting as well. Testing consisted of using predefined known outputs and comparing them to the computer output. Text data is entered into the message field which is then encrypted with a Geffe Generator LFSR and Vernam Cipher.

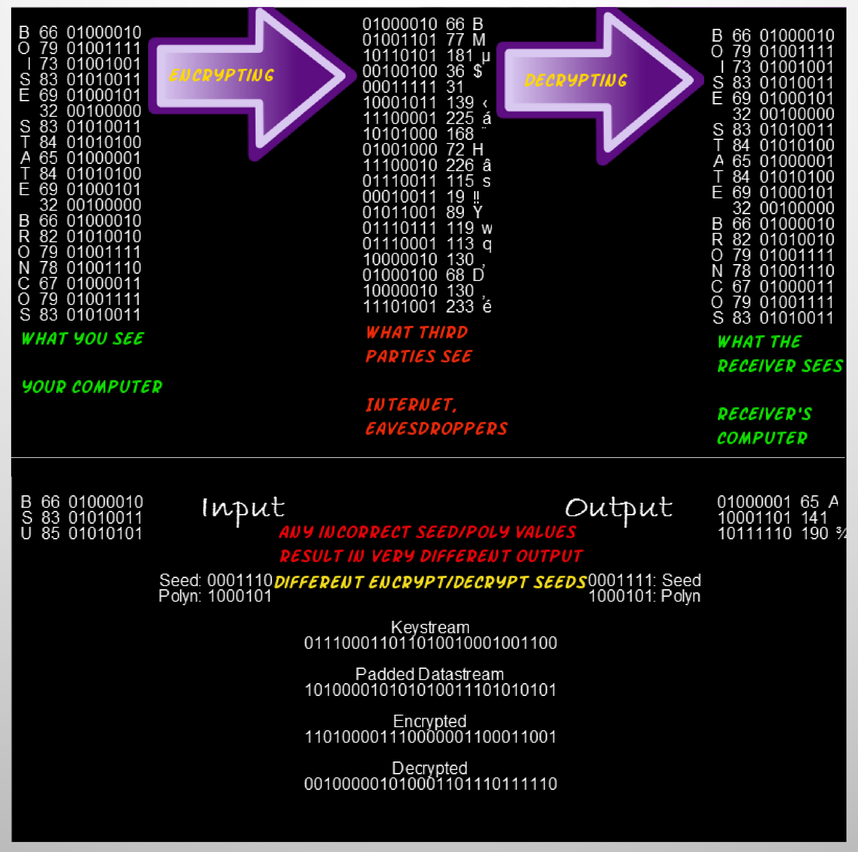
Seed values are encrypted with RSA, to securely send keys used to decrypt messages to the receiver. If someone were to crack a message, a new one being sent would not use the same values as the cracked one.

Results

A RSA key generator (keygen) has been developed that can be used in conjunction with the MP Cryptographer to easily send and decrypt emails. The way the RSA keygen works allows people to generate lists of private and public keys and keep them separate and maintain full privacy.

The MP Cryptographer creates a file that is attached to any email. In the first line of the file, we have the seed values encrypted with RSA, and they are used to decrypt the rest of the file contents. This program is modifiable so that groups may change preset values within the program so that the program will only work with other copies of the same modified MP Cryptographer. You can see a development build of MP Cryptographer at the top right of this poster.

The program will be released as open source so that other developers can learn and use the code under an open source license.

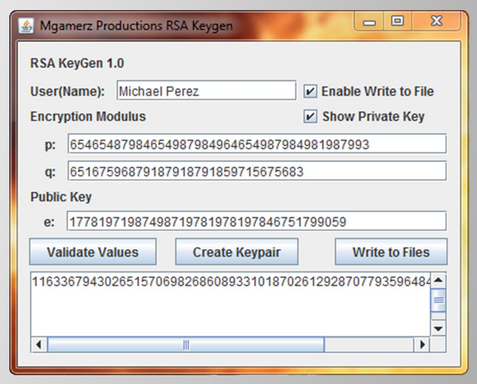


Conclusions/Discussion

Using Linear Feedback Shift Registers in cryptology are essential for many low power devices. When speed is required, LFSRs can greatly enhance speed with only a slight reduction in security if proper steps are taken.

Programs developed in Java and Maple can be used now by people who need to quickly make an RSA key of any length. People can also send secure messages with low end machines that can run Java. Porting code to Java-like systems would not be difficult and would work well on limited systems like Android.

An idea for future implementation of randomness would be to ponder what ways computers can pull random numbers without having to have a complex and expensive system. One idea would be to use the gyroscopes in phones.



Acknowledgements

Partial support for this work was provided by the National Science Foundation's Science, Technology, Engineering, and Mathematics Talent Expansion Program (STEP) under Award No. 0856815 . Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

NATIONAL SCIENCE FOUNDATION

BOISE STATE UNIVERSITY