

Stream Cipher – Programming Directions

Goal: Write VBA code within Microsoft Word or Excel, which will enable a user to encrypt and decrypt using a stream cipher.

- Encryption
 - Inputs
 - Random stream of bits to initialize the LFSR
 - Taps for the LFSR
 - Plaintext
 - Output – ciphertext in binary
- Decryption
 - Inputs
 - Random stream of bits to initialize the LFSR
 - Taps for the LFSR
 - Ciphertext in binary
 - Output – plaintext
- Other things to include
 - Appropriate use of tab in the code (organization).
 - Appropriate documentation (comments) in the code
 - You may not use anyone else’s code or logic in your program. You may use the code provided by Mr. Evans (ASCII to binary function and the LFSR code).
 - Instructions for using the program and a method of launching the VBA code
 - If you are reading and/or writing to a text file, there must be an input for where to write to and what to read from.
- Email
 - Email to: evans@scienceandmathacademy.com
 - Subject: *YourLastName* – Stream
 - Filename: *YourLastName*_stream.doc or *YourLastName*_stream.xls
 - Make sure to cc yourself on the email, (this is your proof that you turned it in on time.)
 - Make sure to include your name in the body of the email and the name of the assignment.

Grading:

Correctly prompts and handles inputs	/6
Properly encrypts a passage using stream cipher	/20
Properly decrypts a passage using stream cipher	/15
Appropriate use of tab (organization)	/2
Appropriate use of documentation	/2
Emails assignment correctly	/1
Instructions and method for launching program	/4
Total	/50