Dr. Janaka Alawatugoda

CO325 Cryptology Assignment (Group Assignment)

Instructions: The aim of this assignment is to lead you to discuss, explore and clearly understand the ideas that we discussed in past few lectures. Therefore, I need to do this as a group assignment. Create a group of 3 members and prepare a document answering the questions. You need to submit hard copies on 4th March during the lecture hours (10AM-12 noon).

1. Perfect Secrecy.
   1.1. What is perfect secrecy?
   1.2. Explain the reason that one-time pad provides perfect secrecy?
   1.3. What are the limitations of one-time pad?
2. What is the similarity between stream ciphers and the one-time pad? What is the difference between stream ciphers and the one-time pad? What is the advantage of stream ciphers over the one-time pad?
   2.1. What are the three basic properties used to measure the strength of a key stream which is generated by a stream cipher?
   2.2. Explain how the attacks can be launched in stream ciphers that have key streams which do not satisfy those properties?
3. What is a maximal length sequence (or m-sequence)?

Theorem

Any m-sequence generated by an LFSR of length n satisfies the following three properties:

1. *its period is* $2^n - 1$
2. *its linear complexity is n*
3. *it is G-random*

3.1. A military troop communicates with their headquarters using a telegraph system. Assume that their plaintext message are at most 5-bits of length. You are asked to design a new stream cipher to encrypt these telegraph messages.

3.1.1. What is the desirable period of the key stream (period > 5 or period < 5) for your stream cipher? Justify your answer.

3.1.2. Explain an easiest way that you could find a sequence with the desirable period (> 5 or < 5) for this stream cipher (hint: Theorem).

3.1.3. What is the shortest desirable period you can find? What is the linear complexity of that sequence (hint: Theorem)?

3.1.4. Write a sequence with the shortest desirable period that you may use, explain why this is desirable (in terms of the length of the period, G-randomness) and explain what is the negative property of this sequence?

3.1.5. Draw the diagram of the LFSR, that generates the sequence you gave, and give the initial vector which constructs the sequence.

3.1.6. Propose a solution to overcome the negative property of the sequence you gave in 3.1.4 (you are asked to use minimum possible LFSRs in the solution).

4. Write a small article on AES considering following facts:

4.1. Small introduction to AES

4.2. Encryption/Decryption processes

4.3. Possible attacks on AES

You may give list of references you used to write this article. This should be around 1.5-2 pages.