Homework – Cryptography Part II

Program 1

Write a program to perform ***Vernam Cipher*** cryptography.

- Inputs
  - A seed value to the random number generator.
  - A way to specify encode or decode. E.g. 0 -> encode, 1 -> decode
  - A string of characters to encode/decode. You may ignore case (e.g. treat upper and lower case characters as identical.) Punctuation and spaces should not be encoded (e.g. pass them through as they are input.)
- Test
  - Use the following values to demonstrate your code:

    Seed: 42

    Encode/Decode: encode

    String: AbC dEf GhI jKl MnO pQr StU vWx Yz
  - Decode test:

    Seed: 42

    Encode/Decode: decode

    String: <use the output from the encode test as the input to the decode test>

Program 2

Write a program to perform ***Book Cipher*** cryptography. Use the ***Vignère Tableu*** as shown on Table 2.1 of the assigned reading for the substitution table. Refer to the section Book Ciphers of the assigned reading for algorithm reference Use the following string as the key:

key = "Anothersourceofsupposedlyrandomnumbersisanybookpieceofmusicorotherobject";

- Inputs
  - A way to specify encode or decode. E.g. 0 -> encode, 1 -> decode

  - A string of characters to encode/decode. You may ignore case (e.g. treat upper and lower case characters as identical.) Punctuation and spaces should not be encoded (e.g. pass them through as they are input.)

- Test
  - Use the following values to demonstrate your code:

    Encode/Decode: encode

    String: AbC dEf GhI jKl MnO pQr StU vWx Yz
  - Decode test:

    Encode/Decode: decode

    String: <use the output from the encode test as the input to the decode test>

Deliverables

- All source code
- Screen shots of running code
- An essay describing successes, difficulties and how you addressed them, an lessons learned.

Documents will be submitted via Blackboard by attaching your document to the assignment. If you use a product other than Microsoft Word (e.g. Apple Pages, Open Document, Google Docs, Word Perfect, etc.) please save your file as a .PDF. Even if you use Microsoft Word, saving as a .PDF is preferred to avoid issues brought about by version differences. Source code for programs should be placed into a ZIP archive file. Attaching source code files directly within Blackboard may cause problems (.java files do not always attach properly due to security settings.) DO NOT SEND ASSIGNMENTS VIA EMAIL. Assignments can only be submitted one time, make sure you get it correct the first time. Late assignments will lose 10%

Notes

- You may use the programming language of your choice.
- You should include comments in your source code files including [at least] your name and a brief description of the program at the top of the source code file.
- Each technique should be contained within its own source file which can contain both encode and decode methods. That is, you should turn in two (2) source code files.
- In all cases you may assume the input string contains only alphabetic characters and whitespace, whitespace may be ignored (passed through without processing.)