

Homework – Cryptography Part I

Program 1

Write a program to perform *Caesar Cipher* cryptography.

- Inputs
 - An integer to specify the number of alphabetic character shifts: negative number specifies left shift, positive number specifies right shift
 - 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
 - Encode test:

Shift: -3

Encode/Decode: encode

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

Shift: -3

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 *Key Permutation* cryptography.

- Inputs
 - A key word to be used to control the permutation.
 - 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:

Key: secretkey

Encode/Decode: encode

String: AbC dEf GhI jKl MnO pQr StU vWx Yz

- Decode test:

Key: secretkey

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.)