CS 380

Homework 3
PHP

Due: Oct 4, 2020, 11:59PM

Below are two options for this assignment. Do one or the other.

Option 1:

Return to the queries from Homework 2. Queries 10, 13 and 14 are quite limited in that they work on exactly one match. Create an interface using PHP that allows users to pick a match (from the set of matches) using an html list selector and a query number (10, 13 or 14). Then execute the selected query on the selected match and return a well-formatted table of the results. You will probably (certainly) need 2 php pages, one that reads the database for the list of matches to select among and one that shows the query results.

What to hand in:

- The URL for the html (or php) page to start into your query.
- A copy of your PHP program(s). This PHP program must be runnable on comet.cs.brynmawr.edu. Realistically, it does not make much sense for it to run anywhere else since the database is also on comet.
- a README file telling me anything I need to know to actually use your program. This readme should also contain a description of what went well / poorly in your efforts.

Option 2:

Background:

For lab 3 you implemented the rot13 cypher. While fun and easy, it is woefully insecure. In this option you will implement a slightly more secure (but still far from secure) cypher; the progressive cypher.

For a progressive cypher, the encryptor/decryptor will need the following:

1. The text to be encrypted/decrypted.
2. The initial step (for rot13 this would be 13)
3. The progression size (for rot13 this would be 0).
4. The progression interval. This has two components
    1. The interval (a number)
    2. The interval definition (is the interval a word, a character, or a specific character).
5. Whether to encrypt or decrypt

For instance, suppose the following settings:

text: abcedfg
initial step: 1
progression size: 1

progression interval: character, 2
encrypt

then the encryption is:

a => (a+1+0) = b to be complete the formula is actually
chr(((ord('abcdefg'[0])-ord('a') +1) mod 26) + ord('a'))
b => (b+1+0) = c
c => (c+1+1) = e (progress by 1 after 2 characters)
d => (d+1+1) = f
e => (e+1+2) = h (progress by 1 after 2 characters)
g => (g+1+2) = i

To decrypt you just subtract rather than add.

For more about progressive cyphers there are innumerable descriptions of progressive cyphers on the web.

Part 1:

Create a html page that has a form which collects all of the above information (note that this page could be generated by PHP). That is:

the text
the initial step
the progression size
the progression step
when to progress

The page should also have the ability to "do the same thing as last time with this text." That is, given the text, it should use the same encryption/decryption parameters as for the previous call (from this browser). You could do this either by filling in the fields in the form is you use PHP to generate the page or by having a checkbox (or the like) on the form that says "repeat" and then having the receiving PHP use the previous inputs. (Or you could do something totally different from my suggestions so long as you accomplish the same end)ß

Part 2:

Create a PHP program (page?) that does encryption/decryption using the parameters from your html page. The system must work on lower case letters and upper case letters. Your encryptor may operate so that, a lower case letter will always be encrypted to another lower case letter and upper to upper. (Better would be to have upper and lower case handled together.) Anything not a lower case or upper case letter should not be encrypted.

The PHP must support the "Do the same things as last time". You should support this using sessions.

The response from the program should be well-formatted html with the encrypted (or decrypted) version of the submitted text.

What to hand in:

- The URL for your html page
- A copy of your PHP program. This PHP program must be runnable on comet.cs.brynmawr.edu
  - At the very least your PHP must be able to decrypt anything that is can encrypt. So if you PHP is able to encrypt with word based stepping, it should decrypt that also.

- a README file telling me anything I need to know to actually use your program. This readme should also contain a description of what went well / poorly in your efforts.