Vigenere Square Substitution Cipher Task Sheet

November 17, 2014

Name:

1. Turn on your computer and go to the following website: http://5010.mathed.usu.edu/Fall2014/KKing/menu2index.html
2. Read the directions on the website. The paragraphs above the applet gives a little background to the Vigenere Square Substitution Cipher.
3. Think of a word or a phrase. This will become what is known as the Keyword or Key phrase. Delete any repeating letters and any spaces within your keyword or phrase. (ex. If I chose the key phrase "hello moto" I would delete any repeating letters and the space, so my key word would become "HELOMT") Write your keyword or key phrase below:
4. Note that on the left side of the applet, there is a list of letters in a red box entitled "Keyword letters." Checking a box next to a letter will highlight the row corresponding to that letter in the keyword. Also note that on the right side of the applet, there is a list of letters in a green box entitled "Plaintext letters." Checking a box next to a letter will highlight the column corresponding to that letter in the plaintext.
5. We want to encipher the plaintext message "Army attack." Our first step is to write the message down. Write the plaintext message "Army attack" down with a little space between each letter.:

   Plaintext: A r m y a t t a c k

   Keyword:
6. Now, underneath the plaintext message you just wrote, write the keyword. Write the key word such that every letter in the plaintext message corresponds to one letter in the keyword. (Note, when you come to the end of your keyword, simply repeat it so it spans the length of the plaintext message.) Example:

   Plaintext: A r m y a t t a c k

   Keyword: h e l o m t h e l o
7. Now, note that I have the plaintext letter "A" and the keyword letter "h." (you may have a different keyword letter corresponding to the A in Army). In the applet, in the red keyword letter box, check h (or whatever letter you have that corresponds with the A in Army). In the green plaintext letter box, check A. Where the two rectangles intercept is my ciphertext letter. For me, this letter is H. For the next letter, I would check the R in the green plaintext box and the E in the red keyword box. My ciphertext would be V.
8. Continue this pattern until you reach the full ciphertext. With the Keyword "HELOMT" the plaintext message "Army attack" enciphers to the ciphertext "HVXM TFMENY". Write your ciphertext below:
9. What are at least 2 advantages of the Vigenere Square Cipher over a monoalphabetic substitution cipher such as a Caesar shift cipher? Are there any disadvantages to using this cipher?
10. If you knew the keyword used to encipher a message, and you were given the ciphertext, how would you decipher the ciphertext to give you the original plaintext?