Assignment 1: Symmetric Crypto

Secure Programming

Strict deadline: November 12, 2018

Question 1 (10 points)

Implement the Playfair cipher in Python 2 (not Python 3). See the slides or https://en.wikipedia.org/wiki/Playfair_cipher for example inputs and outputs. Note that the Wikipedia page mentions several variants of Playfair. In your implementation, please replace occurrences of I with J and use X for padding.

The program should take two command line options: a key and a plaintext/ciphertext message (plaintext consists of ASCII English letters only). Additionally, add a command line option that tells the program whether it should use encryption or decryption mode. The program should print the plaintext/ciphertext resulting from the decryption/encryption to screen. You may assume that the plaintext input does not contain the padding character X.

Example usage:

- Encrypting a message <plaintext> with <key> (should print the ciphertext to stdout):
  ./playfair.py -e <key> <plaintext>
- Decrypting a message <ciphertext> with <key> (should print the plaintext to stdout):
  ./playfair.py -d <key> <ciphertext>

Your program should support the use of a key shorter than 25 characters. In that case, it should pad the key with the remaining letters of the alphabet (except i), in order. For example, if the key is "crypto," then the remaining 19 (i.e., 25-6) characters will be "abdefghjklmnqsuvwxz," and the full key will be "cryptoabdfghjklmnopquvwxz." The output of the decryption should drop any remaining padding characters. That is, decrypted messages should not contain the letter X.

Note: Only solutions implemented in Python 2 will be accepted. Using any library that implements Playfair will result in a score of zero points. We will apply standard checks for plagiarism.

Question 2 (5 points)

Is there any secure way to solve the key distribution problem faced in symmetric-key crypto systems using only concepts discussed in the lectures up to and including symmetric cryptography (i.e., without using any concepts from assymetric crypto systems)? If so, describe how. If not, explain why not.

How to Submit

To hand in the assignment, submit a zip file on Canvas called <your vunet id>.zip that contains:

- Your Python source file for Question 1, named playfair.py. Your Python source should contain clear comments describing your implementation decisions. Your program must use the exact input/output interface described above. Please include your name, student number, Vunet ID, and e-mail address in a comment at the top of the file.
- A txt, doc(x), pdf, or odt file containing your answer to Question 2. The filename must be "question2," as in "question2.pdf." We prefer plain txt or pdf files. Please include your name, student number, Vunet ID, and e-mail address at the top of the document.