Assignment 1

Due Friday, September 28th, 2019 at 23:59

Assignments are to be completed individually. We generally expect you to make an honest effort searching around online before contacting course staff with technical questions (`stackexchange.com` and `crypto.stackexchange.com` are great resources btw).

Submission Instructions

Please use common document file formats such as `.txt`, `.pdf`, `.doc`, etc. Place your answers into separate files and/or subfolders for each of the 4 questions. Submit a `.zip` of the assignment files via OWL. The submission form in OWL will be available only up to 48 hours after the assignment due date. Email submissions are not accepted. Be sure to consult the course outline regarding the late policy.

1. [4 marks] Encryption Basics

For each of the following, state whether the given ciphertext is a valid encryption under the given cipher. Your answer should be of the form: *Yes*, *No*, or *Insufficient information*, followed by a one or two sentence justification. .

(a) [1 marks] You've intercepted an Engima encrypted message from a rival engineering school. The ciphertext ends with: `flvhfgegkwogaggvxzwk`. You know from past intercepts that plaintexts always end with the university's name, and are padded with `x`'s to prevent length-based cryptanalysis. Which of the following schools wrote the message? Explain your answer.

- `mcmasteruniversityxx`
- `queensuniversityxxxx`
- `mcgilluniversityxxxx`
- `universitedemontreal`
- `universityofcalgaryx`
- `universityofalbertax`
- `universityofwaterloo`
- `universityoftorontox`

(b) [1 marks] Assuming the ciphertext from the previous questions was created using a one-time pad, which univsity would be responsible? Explain your answer.

(c) [1 marks] Let x ={0xF2, 0x14, 0x72, 0xA9, 0x30, 0x4b, 0x03, 0xC1 } be a vector of bytes. Is x a valid DES ciphertext?[1]

(d) [1 marks] Let b={0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF} be a vector of bytes. Is b a valid AES ciphertext? Why or why not?

2. [3 marks] Security Games

For each of the following, use the appropriate security game to prove the given cipher is insecure under the stated security notion.

(a) [1 marks] Prove that Enigma is not IND-EAV secure.

(b) [1 marks] Prove that AES in CBC mode is not IND-CPA secure if the IV can be predicted by the adversary.

(c) [1 marks] Prove that AES in CBC mode in not IND-CCA2 secure, even if the adversary cannot predict the IV.

Note: You don't have to be formal. The goal here is to convince us that you understand the mechanics of these security games, can come up with a strategy for the adversary to follow, and then justify why that strategy gives them a non-negligible advantage.

3. [2 marks] Encryption in Practice

For this question you will explore encryption in practice. This is a somewhat open-ended problem and you will be graded according to your ability to make good security-conscious choices. Marks will be deducted if anyone (beyond the intended recipient) could recover information about the plaintext in less work than brute-force.

The plaintext shall consist of your full name and student number. Encrypt it using 128-bit AES in CBC mode. Use any method (*i.e.,* programming language or software program) you wish. Encode characters in ASCII (e.g., the character '0' is encoded as the byte 0x30, 'A' as 0x41, etc).

Submit the following:

(a) A text file containing the source code or commands you used. In the comments, specify your name, student number, what programming language, library, or software program you used,

[1] Note: The prefix 0x... denotes a hexidecimal value.

(b) A text file containing the exact plaintext message (i.e., name and student number),

(c) The encryption key used, written as a list of hexidecimal bytes (e.g., `00, 01, 02, ...EE, FF`),

(d) Any initialization vector (IV) used, written as a list of hexidecimal bytes,

(e) The resulting ciphertext, written as a list of hexidecimal bytes.