

EE 4215 –Security Technology – Spring 2018/19

Assignment 1 – Due date: February 17, 2019 – mid-night

Electronic submission only on Canvas

Name: _____

Date: _____

Student ID: _____

Mark: _____

Submission guidelines:

- Please prepare your assignment in “PDF” format.
- For observe the departmental rules for late submission (i.e. 50% deduction per day).

Security Management

- 1) To save cost, your company is going to use Google Apps Email to replace your company’s email server. Perform a risk assessment by identifying assets, threats, vulnerabilities and their impact and likelihood of occurrence, possible countermeasures/controls.

Based on your risk assessment, would you recommend your company to switch to Google Apps Email service? Why?

Ans: Based on your risk assessment, both sides are acceptable. **All aspects** (assets, threats, vulnerabilities, impact and so on) need be identified.

- 2) Describe in your own words the definition of the following key security terminologies:
 - a) Passive attack,
 - b) Active attack,
 - c) Access control,
 - d) Data confidentiality,
 - e) Data Integrity,
 - f) non-repudiation.

Ans: You can find the above concepts from Lecture note 1.

Technical Tools

- 3) DES question – Please visit this URL:
https://www.tools4noobs.com/online_tools/encrypt/
For the plaintext, please key-in “EE4215” as the input data, for the key, please enter your student ID.
 - a) What is the resulting ciphertext (in Hexadecimal)? How many bytes are there and why?

Ans: Based on your key, you may have different answers, but the length should be the same. The length is **8 bytes**. That’s because in DES, the block size is 64 bits.

b) Briefly describe what computations have been involved.

Ans: Describe the framework of DES and in each Feistel round, describe expansion P-box, S-box, XOR and straight P-box.

c) Repeat the same task, with another encryption, Rijndael-128.

Ans: Answer (a) and (b) for Rijndael-128 again. The block size of Rijndael-128 is 128 bits (16 bytes). Describe SubBytes, ShiftRows, MixColumns and AddRoundKeys.

4) Get familiar with the tool **Openssl** (<http://www.openssl.org/>).

a) Give a screen dump to show that you can have installed the package by running the command
openssl version -a

b) The following ciphertext was captured and it was suspected that it was encrypted with DES and the key is "pass" (without the quote ""):
U2FsdGVkX18ztmw81FTK/c+jAf8xtcZdlpesuV2PLDM=

Find the plaintext using Openssl and provide a screen-dump as evidence in this assignment.

Ans: openssl enc -des -d -a -in cipher.txt -out plaintext.txt

5) Based on the Sage example in the lecture notes about CaesarEncrypt() and CaesarDecrypt(), in this question, you need to write a brute force attack function on Sage that can decrypt any Caesar ciphertext.

def BruteForceAttack(ciphertext):

For the output of this function, you are expected to handle ciphertext for any length, and output all the possible plaintext.

What would be the original plaintext of this ciphertext?
"y byau heej ruuh vbeqji."

Ans: The original plaintext is "I like root beer floats".

Mathematics

6) Classic cipher question – Vigenere cipher

Given the following ciphertext:

COGMEIKQGRDAQXNBFFGCWCVDDNDBQEVTBDVULGHIEAB

Find the key that yields the following plaintext: (throw away the blanks)

MR MUSTARD WITH THE CANDLESTICK IN THE HALL

Ans: If throw away the last characters, the ciphertext is:

COGMEIKQGRDAQXNBFFGCWCVDDNDBQEVTBDVU

The answer is:

QXUSMPKZDVVHJEGXDFTZLYDKVLTTDLOPUDKJ

7) Use the extended Euclidean algorithm, find the multiplicative inverse of:

a) $1234 \bmod 4321$

b) $550 \bmod 1769$

Ans: (a) $1234 \bmod 4321$, $4321 = 1234 \cdot 3 + 619$, $1234 = 619 \cdot 1 + 615$,
 $619 = 615 \cdot 1 + 4$, $615 = 4 \cdot 153 + 3$, $4 = 3 \cdot 1 + 1$, $1 = 4 \cdot 1 + 3 \cdot (-1) = 4321 \cdot 309 + 1234 \cdot (-1082)$, $\text{ans} = 4321 - 1082 = 3239$
(b) similarly, $\text{ans} = 550$

~ END ~