14-741/18-631: Homework 1

All sections (A/B/J/SV) Due: Wednesday September 26, 2018 by 2:30pm EST

Name:

Andrew ID:

Scores

Problem 1 (15 pts max):

Problem 2 (5 pts max):

Problem 3 (10 pts max):

Problem 4 (15 pts max):

Problem 5 (20 pts max):

Problem 6 (25 pts max):

Problem 7 (10 pts max):

Total (100 pts max):

Guidelines:

- Be neat and concise in your explanations.
- You must use exactly one page for your explanation for each Problem (code you wrote may be on additional pages).
- Please check your English. You won't be penalized for using incorrect grammar, but you will get penalized if we can't understand what you are writing.
- Proofs (including mathematical proofs) get full credit. Statements without proof or argumentation get no credit.
- There is an old saying from one of my math teachers in college: "In math, anything partially right is totally wrong." While we are not as loathe to give partial credit, please check your derivations.
- **This is not a group assignment. Feel free to discuss the assignment in general terms with other people, but the answers must be your own.** Our academic integrity policy strictly follows the current INI Student Handbook `http://www.ini.cmu.edu/current_students/handbook/`, section IV-C.
- Write a report using your favorite editor **Only PDF submissions will be graded.**
- Submit to Gradescope a PDF file containing your explanations and your code files before 2:30pm Eastern on the due date. Late submissions incur penalties as described on the syllabus (first you use up grace credits, then you lose points).
- Post any clarifications or questions regarding this homework to Piazza.
- Good luck!

1 Using PGP (15 points)

Create a public/private OpenPGP key pair, using, for instance the GNU Privacy Guard (*gpg*), or similar package. Give us the key fingerprint in writing in your assignment handout.

Our email address is ta18631@gmx.com. The OpenPGP keyID is 6FC8F0B4FE1316C8, the fingerprint is 285A FF84 0FD9 DD19 5E09 E9DC 6FC8 F0B4 FE13 16C8, and the public key is available on `https://pgp.mit.edu/`.

1. Based on this information, how do you verify that the public key you got from the web page is valid, i.e., that no one has modified it?

2. Send us three emails as follows:

   (a) An email with the subject "Homework 1 PGP exercise 1", and a body containing "Hello! This is signed." and your name. The email should be signed with your private key, but not encrypted.

   (b) An email with the subject "Homework 1 PGP exercise 2", and a body containing "Hello! This is encrypted." and your name. The email should be encrypted so that only I can read it, but shouldn't be signed.

   (c) An email with the subject "Homework 1 PGP exercise 3", and a body containing "Hello! This is encrypted and signed." and your name. The email should be encrypted so that only I can read it, and signed with your private key.

   You can use either PGP/MIME or PGP/inline – it's up to you.

   Important note: You have **one shot** at this. Only your first attempt for each email will be considered. No exceptions.

3. If you had to send us an attachment, would you use PGP/MIME or PGP/inline, knowing that the various email client(s) we use support both methods? Justify your answer.

Hint: These webpages may be of interest:

- `http://www.bretschneidernet.de/tips/secmua.html` (In German, but the important thing, the table, is quite self-explanatory.)
- `http://www.gnupg.org/` - the GNU privacy guard homepage
- `http://enigmail.mozdev.org/` for those of you using Mozilla Thunderbird.
- `http://www.mutt.org` for those of you under UNIX.

2 Breaking Vigenere (5 points)

The Vigenere cipher was considered unbreakable for centuries. Now it is easily cracked online! Log into the 14741 CTF Server. Create an SSH proxy tunnel to ctf.martincarlisle.com using the provided directions from Canvas.

Configure your browser to use this proxy, then create an account. You can pick any username you want (so your classmates don't know who you are), but please enter your correct name when you register (visible to instructors only). You must also let us know what your username is in your writeups. After you register, click on the lightning bolt in the upper right corner. You should see a section that says Class Membership. If you don't see that, please click top left icon that says "CTF Placeholder", log back in and you should now see the Class Membership section after clicking the lightning bolt. Join the class 14741 with teacher username thedoctor.

Do not use the webshell. Copy/pasting is hard. Follow the directions provided on Canvas to ssh to the server.

To connect to a network service, you can use netcat (nc). For example, "nc 192.168.2.63 80" would connect to a service running on port 80. If you want to solve a problem with Python, here's some simple Python code to get started:

```
#!/usr/bin/python           # This is client.py file

import socket               # Import socket module

s = socket.socket()         # Create a socket object
host = "192.168.2.63"       # Remote machine name
port = 12345                # Remote port

s.connect((host, port))
print s.recv(1024)
s.close() # Close the socket when done
```

Solve the Vigenere problem.

Submit a writeup containing your CTF username, and what steps you used to solve this problem.

3 Two-time pads (10 points)

A one-time pad is unbreakable crypto, but what happens if you reuse the pad? Solve the twotime problem on the 14741 CTF Server. Submit a writeup containing your CTF username and what steps you used to solve the problem.

4 ECB (15 points)

Why is it bad to use ECB mode with block cryptography? Solve the ECB problem on the 14741 CTF Server. Submit a writeup containing your CTF username and what steps you used to solve the problem.

5 RSA (20 points)

RSA public key cryptography depends on it being computationally hard to factor the product of two large primes. What happens if you can make the search space a lot smaller? Solve the RSA problem on the 14741 CTF Server. Submit a writeup containing your CTF username and what steps you used to solve the problem.

6 Padding attacks (25 points)

Preliminaries

PKCS#7 Padding AES is a block cipher based algorithm, which operates on 128 bit blocks (16 byte blocks) with a 128 bit key. AES requires padding to make plaintext in multiple of 16 bytes (padding is required even if the plaintext length is already multiple of 16 for avoiding ambiguity).

The PKCS#7 padding scheme is a simple padding algorithm: Calculate $b = 16 - (\mathsf{length}(plain) \bmod 16)$ then append b number of byte b to the plaintext. Below are examples of valid padding in hex representation:

"XXXXXXXXABC" requires 5 bytes padding: 414243**0505050505**
"XXXXXXXXABCDEF" requires 2 bytes padding: 41424344454**60202**
"XXXXXXXXABCDEFGH" requires 16 bytes padding: 4142434445464748**10101010101010101010101010101010**

Cipher Block Chaining (CBC) Mode As a block cipher algorithm, AES operates on blocks. The input string will be divided into multiple 16 byte blocks prior to encrypting or decrypting. Mathematical formulas for CBC are:

$$\begin{aligned} C_i &= \mathsf{Enc}(P_i \oplus C_{i-1}) \\ P_i &= \mathsf{Dec}(C_i) \oplus C_{i-1} \\ C_i &= i_{th} \text{ block of ciphertext } (C_0 \text{ is IV, first ciphertext block is } C_1) \\ P_i &= i_{th} \text{ block of plaintext (first plaintext block is } P_1) \end{aligned}$$

Decryption Attack In the decryption formula, attacker controls C_{i-1} and wants to learn $\mathsf{Dec}(C_i)$. So the mathematical formula is: $\mathsf{Dec}(C_i) = C_{i-1} \oplus P_i$. Attacker doesn't know P_i but the attacker knows whether P_i has valid or invalid padding using an Oracle.

Encryption Attack In this attack, the attacker controls both C_i and C_{i-1}. Once attacker learns $\mathsf{Dec}(C_i)$ using decryption attack, the attacker can make any text P_i with the formula: $P_i = \mathsf{Dec}(C_i) \oplus C_{i-1}$.

Solve the PKCS7 problem on the 14741 CTF Server. Submit a writeup containing your CTF username, and what steps you used to solve this problem.

7 STRIDE Analysis (10 points)

You work for a power company. Currently, your customers have analog readers that meter readers manually visit and record the amount of power consumed once per month. Your boss would like to replace these with ”smart meters” that are connected to the internet and communicate directly, eliminating the cost of meter readers! You have been asked to perform a STRIDE analysis. For each of the categories, identify at least 1 possible threat.