IEMS5710A Fall 2024 - Assignment #1

Due: 12 Nov 2024

Instructions:

- Submit a zip file to the Blackboard that compresses your written answer in a pdf, and your source code files if there is any.
- This assignment takes 30% of the course total.
- For some questions, you may want to install a Ubuntu VM or set up WSL.

1. Consider the non-shadowed entry in a Linux machine below.

```
sha256:$1$sha512$HtQTtdEaQhsBlwP2gJZpO/:500:600:::
```

a) What is the username?
b) What is the hash/encryption method used?
c) What is the salt used?

2. Suppose we are going to encrypt a 10-byte file using AES128 in CBC mode, padding with PKCS#7.

a) What is the ciphertext size?
b) How many padding bytes are there?
c) What is the content of each padding byte?

3. Is there a full period for each of the following LCGs? Explain your answer.

a) m = 32, a = 9, c = 0
b) m = 32, a = 9, c = 2
c) m = 32, a = 9, c = 3

4. An attacker eavesdropped a public key file in PKCS#1 format along with ciphertext encrypted using the RSA algorithm. Try to decode the plaintext, and show your steps. (*Hint:* Use openssl rsa -pubin -in public.pem -text -noout to parse the public key file)

public.pem:

```
-----BEGIN PUBLIC KEY-----
MCQwDQYJKoZIhvcNAQEBBQADEwAwEAIJBWvHrU2oMxbbAgMBAAE=
-----END PUBLIC KEY-----
```

Ciphertext:

```
AxMh6FqZ4mdV
```

5. Assume that Alice encrypted a bit string by the following steps:
    - Use plaintext as the seed to set up a Linear Congruential Generator (LCG);
    - Use Z_{10} generated from the LCG as the ciphertext

However, Eve knows the parameters of the LCG and eavesdropped on the ciphertext. Can Eve decrypt the message? Show the steps.
(Hint: you can use python library Crypto.Util.number.long_to_bytes to check the message)

Evasdropped Parameters:
a=28156751752533189148781084609481693052018897368920147593870294063111 67
c=19047281210962643842930520235735906787998689156966385824308463695377 91
m=19840225221775090054841381281767739429145838595399063133973243989334 53
ciphertext=17156105787398140700017746933118844336466132129557776365172694340002 29