**Fall 2019**
**CS134: Computer and Network Security**
**Homework 2**
**Due: 11/20/19: 11:59pm**

**Full Name:**
**UCI ID Number:**
**Sources:**

**Guidelines:**

- Use any word processor (or handwrite and scan your answers). Upload your solutions **in PDF** to Gradescope.
- No collaboration is allowed. The only people you may consult are the TA-s and the instructor.
- Looking up, paraphrasing or copying answers from the Internet or other sources is not allowed; doing so is a violation of academic honesty. You must cite any sources you use, e.g., reference books, Wikipedia, etc.

**Warning:** any submissions not following the above guidelines will receive a score of zero.

| P1 | P2 | P3 | P4 | P5 | Total |
|---|---|---|---|---|---|
| /30 | /10 | /30 | /10 | /20 | /100 |

**Problem 1: RSA**
Assume the following RSA parameters:

$$p = 7, q = 17, d = 35, c = 9$$

(a) Use Chinese Remainder Theorem to find the value of plaintext $m$. Show your work.

(b) Use Extended Euclidean Algorithm to find the value of public exponent $e$. Show your work.

**NOTE:** Be sure to show your steps clearly. Just showing $m$ and $e$ will be result in zero points.

---

**Solution:**

**Problem 2: Zero-Knowledge with Fizz and Buzz**

You and Alice have stumbled upon two unlabeled bottles of lemonade and a bunch of empty cups. Alice insists that the bottles contain the same type of lemonade, but you know better: you know by taste that one is Fizz and the other Buzz. How could you prove to your friend that lemonades are different, without revealing which is Fizz and which is Buzz? You may assume that the bottles of lemonade will never run out.

---

**Solution:**

**Problem 3: Randomness in ElGamal**

Suppose that, instead of choosing $r$ completely at random in ElGamal public key encryption, a lazy encryptor (Alice) derives it by following $r' = 2r$. Suppose also that Eve knows that Alice had encrypted the same message $m$ with the two random numbers $r$ and $r' = 2r$, thus creating two ciphertexts $\{k,\ c\}$ and $\{k',\ c'\}$. Answer the following questions.

(a) Show how Eve can derive the message $m$ using the two ciphertexts and the public key provided by Alice. Recall that $y = b^x \bmod p,\ k = b^r \bmod p,\ c = m \times y^r \bmod p$.

(b) Show that the attack you have shown in part (a) will work by using the following numbers: $p = 11,\ b = 2,\ x = 3,\ m = 7,\ r = 2$.

---

**Solution:**

**Problem 4: Randomness in Fiat-Shamir**
Recall that in the Fiat-Shamir identification protocol, the prover ($Prv$) chooses a random number $R$ each time $Prv$ wants to prove his identitiy to the verifier ($Ver$). Explain what happens if $Prv$ reuses $R$ and $Ver$ somehow knows about it. Will it enable $Ver$ to obain any information regarding $Prv$'s secret key $S$? Why or why not? Justify your answer.

**NOTE:** Answer to the problem in 3 to 5 lines (including the justification). An answer without a justification will result with an automatic 0.

---

**Solution:**

**Problem 5: Access Control**

Consider a small company that is implementing access control policies on its internally shared files. There are 1500 employees in the company, and 20,000 files initially. The allowed actions on the files are Read (R), Write (W), Execute (E), and Delete (D). On average, 100 files are created every week, each with fewer than 100 employees having access.

(a) Show or describe what an access control matrix would look like for this system.

(b) Show or describe what an access control list would look like for this system.

(c) In terms of storage, would an access control matrix or access control list be better in this system? Why?

(d) Would an ACM or ACL be better in terms of file access time for the employees? (i.e., the time required for the system to check if an employee is authorized to perform an action on a file) Why?

**NOTE:** Limit your answers to five lines each (but you may draw diagrams for parts (a) and (b)). For (a) and (b) you may assume all employees only have read (R) access to all files for simplicity.

---

**Solution:**