Homework 1 (Module 1 and Module 2)

CPE449/549; University of Alabama in Huntsville

Submission Guideline: Please submit answers in PDF or doc format. **Submission Deadline:** September 16.

1. Calculate password entropy for the following passwords (use ASCII characters): password, Password, P@ssw0rd, qwerty, UAH123, MrP*MathPage, 123456, footBall, footb@ll, P33e=7a*E6m. Hint: use $E=\log_2 R^L$, where R=pool of unique charatcers, L=number of characters in your password. For example, for "UAH", R=26 and L=3. For Uah, R=52, and L=3. **Undergraduate students (i.e., CPE449) must calculate any five passwords' entropy, and graduate students must answer all of them. ASCII has 32 special characters.**
2. Write down the major difference between the dictionary attack and rainbow table attack? How can these attacks be prevented?
3. In cybersecurity, what does CIA stand for? Discuss them.
4. Bob is buying a textbook from UAH bookstore. The bill was supposed to be $32.00. However, he finds that the price can be changed to $2.00. Which part of the CIA triad has broken?
5. Ali has taken her final exam and is waiting to get her results by email. By accident, Ali's results are sent to Jason. Which part of the CIA triad has broken?
6. Bob cannot make a call using his cell phone because he kept his cell phone in a hot place. Which part of the CIA triad has broken?
7. What's rainbow table? Suppose a system consists of one especial character, at least one small letters, and at least one numbers. The password can not contain upper case letters. How much space do we need to develop a rainbow table? The system uses SHA512 hash function. Assume that the passwords are 8-bit long.
8. MD5 and SHA 256 are used to hash passwords. Which hashing algorithm will take more space to build a rainbow table. Which one will you use?

Question	Mark Distribution	Rubric if any	Graded Points
1	02 points per password for graduate students. 04 points per password for undergraduate students. Total points: 20.	0 points for wrong answers and full points for correct answers.	
2	10+10		
3	2+8		
4	5	0 points for wrong answers	
5	5	0 points for wrong answers	
6		0 points for wrong answers	
7	5+15	0 points for wrong answers and full points for correct answers, and 50% points for wrong calculation.	
8	15+5	0 points for wrong answers	