Homework #1

CSE 7339. Computer System Security

**[Mark D. Hoffman](mailto:mhoffman@smu.edu)**

Please submit under the Homework #1 link on the Assignments page of Canvas. Unless otherwise stated, **PLEASE SHOW ALL WORK** and try to only use classmate assistance as a last ditch effort**.**

**Question 1 – Auth-what?**

**Discuss the difference between Authentication and Authorization.**

**Question 2 – What is the plain text of a Substitution Cipher?**

1. **Using a Caesar Cipher with a key of 3 (shift by 3), what is the plaintext if the cipher text is FUBSWRJUDSKB FDQ EH IXQ? Work by hand and show all work. HINT: If your solution is nonsense, it is probably incorrect.**
2. **Using any means available (Google is your friend), solve the following Substitution Cipher with an unknown key of a random alphabet:**

1. **Find the plaintext if the cipher text is**

EXUYGJMJAUVZV ZV RCGWM BZCCZENAG

1. **Explain with enough detail to duplicate your method how you solved this:**

**Question 3 – Transposition ciphers:**

1. **Solve the following Grille cipher using the included cut out. Briefly describe your method of breaking the cipher.**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| R | H | K | T |  |  |  |  |  |
| U | S | B | D |  |  |  |  |  |
| O | C | E | E |  |  |  |  |  |
| Y | E | O | O |  |  |  |  |  |

1. **Solve the following Double Transposition cipher. Briefly describe your method of breaking the cipher.**

|  |  |  |  |
| --- | --- | --- | --- |
| O | S | E | D |
| T | C | E | H |
| R | E | K | O |
| Y | B | U | O |

**Question 4 - What is the one-time pad for encryption?**

**Using the letter encoding below discussed in class (along with one-time pad using XOR), the cipher text, KITLKE was generated using one-time pad.**

**E = 000 H = 001 I = 010 K = 011 L = 100 R = 101 S = 110 T = 111**

1. **What is the one time pad used if the plain text is “thrill”?**
2. **What is the key if the plain text was “tiller”?**

**Question 5 - Solve the following Null Cipher (you do not need to show work or describe how you solved this, but understanding how the answer is derived is still important):**

BOB RUNS EVERY AFTERNOON. KAREN IS NOT GOING. CARL ONCE DROVE EVERY SUNDAY. IRENE SAW HELEN AND ROBERT DANCE.