Homework #1
CSE 7339 Computer System Security
Mark D. Hoffman

Name: Bingying Liang
ID: 48999397

Sep 9 2023

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

1. **Question 1 – Auth-what?**
   Discuss the difference between Authentication and Authorization.

   Solution:
   Authentication: is the process of verifying the identity of an individual, system, or application. It's essentially answering the question, "Are you who you say you are?"
   Example: Passwords, Biometrics

   Authorization: Once authentication is established, authorization is the process of granting or denying access to specific resources based on that identity. It's essentially answering the question, "What are you allowed to do or see?"
   Example: Access Control Lists/Capabilities; Multilevel security (MLS), security modeling, convert channel, inference control; Firewalls, intrusion detection (IDS)

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

   (a) 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.

   Solution:

   Plaintext: ABCDEFGHIJKLMNOPQRSTUVWXYZ
   Ciphertext: XYZABCDEFGHIJKLMNOPQRSTUVW

   Therefore, "FUBSWRJUDSKB FDQ EH IXQ" $\rightarrow$ "cryptography can be fun".

   (b) Using any means available (Google is your friend), solve the following Substitution Cipher with an unknown key of a random alphabet:

      i. Find the plaintext if the cipher text is

      EXUYGJMJAUVZV ZV RCGWM BZCCZENAG

      Solution: cryptanalysis is often difficult

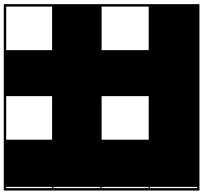
      ii. Explain with enough detail to duplicate your method how you solved this:

      Solution: Used the website https://quipqiup.com/, it can solve simple substitution ciphers often found in newspapers, including puzzles like cryptoquips (in which word boundaries are preserved) and patristocrats (inwhi chwor dboun darie saren t). I chose the "statistics" bottom to help me solve the problem.

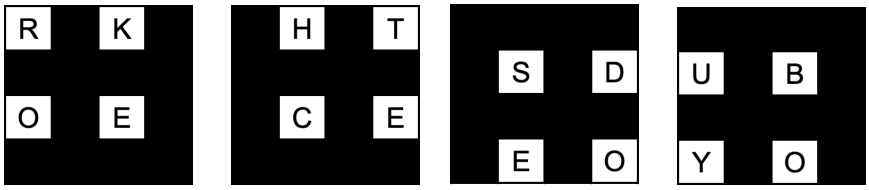
3. **Question 3 – Transposition ciphers:**

   (a) 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



Solution:



(a) (b) (c) (d)

(a) rotate $0°$ (b) rotate $90°$ (c) rotate $180°$ (d) rotate $270°$

If the reading order is from ROKE, then (b) will be THEC, (c) ODES, (d) YOUB, and then combine then in order (d)(a)(b)(c), will get "YOUBROKETHECODES".

(b) 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

Solution:

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

(a)

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

(b)

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

(c)

(a) swap col(2, 4) (b) swap row(1,4) (c) swap row(2,3)

	col1	col2	col3	col4
row1	O	S	E	D
row2	T	C	E	H
row3	R	E	K	O
row4	Y	B	U	O

$\rightarrow$

	col1	col4	col3	col2
row4	Y	O	U	B
row3	R	O	K	E
row2	T	H	E	C
row1	O	D	E	S

Therefore, the plaintext is "YOUBROKETHECODES". The final key is (4,3,2,1) and (1,4,3,2). The website https://www.boxentriq.com/code-breaking/double-transposition-cipher also can solve this. "you broke the codes".

4. **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

(a) What is the one time pad used if the plain text is "thrill"?

Solution:

Plaintext:	t	h	r	i	l	l
Encoded Plaintext:	111	001	101	010	100	100
Ciphertext:	K	I	T	L	K	E
Encoded Ciphertext:	011	010	111	100	011	000
Encoded Pad:	100	011	010	110	111	100
Pad:	L	K	I	S	T	L

Therefore, one time pad is "100 011 010 110 111 100" or "lkistl"

(b) What is the key if the plain text was "tiller"?

Solution:

Plaintext:	t	i	l	l	e	r
Encoded Plaintext:	111	010	100	100	000	101
Ciphertext:	K	I	T	L	K	E
Encoded Ciphertext:	011	010	111	100	011	000
Encoded Key:	100	000	011	000	011	101
Key:	L	E	K	E	K	R

Therefore, key is "100 001 101 010 100 100" or "lekekr".

5. **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.

Solution: Taking the first letter of each word in the message:

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

Therefore, "BREAKINGCODESISHARD"