Homework #1

Robert Rash
Class: CSE5339
Section: 001C

10 September 2017

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

   Authentication is ensuring that a user is who they say they are, whereas authorization is enforcing restrictions on a user who is already authenticated.

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 ciphertext is FUBSWRJUDSKB FDQ EH IXQ? Work by hand and show all work. Hint: If your solution is nonsense, it is probably incorrect.**

   Since we know the shift number, there are only two possible directions to shift: left or right. Knowing that, I've listed the two possible plaintexts in the table below.

plaintext 1	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w
ciphertext	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
plaintext 2	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c

   Since the words of the ciphertext are space-delineated, we can choose one of the smaller words to attempt to decrypt in order to make our lives easier. For this case, I'm going to choose the word "FDQ" from the ciphertext.

   Using plaintext 1: FDQ → CAN
   Using plaintext 2: FDQ → IGT

   Since plaintext 1 leaves us with a valid English word, it leads me to believe that it is likely the correct answer.

   Decrypted:
   FUBSWRJUDSKB FDQ EH IXQ → CRYPTOGRAPHY CAN BE FUN

   (b) **Using any means available (Google is your friend) on a Substitution Cipher with an unknown key of a random alphabet:**

      i. **Find the plaintext if the cipher text is:** EXUYGJMJAUVZV ZV RCGWM BZCCZENAG

      Ciphertext: EXUYGJMJAUVZV ZV RCGWM BZCCZENAG
      Plaintext: CRYPTANALYSIS IS OFTEN DIFFICULT

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

      Using the website https://quipqiup.com, one can type in ciphertext and the website will generate a list of possible plaintext solutions. In this instance, the fact that the ciphertext was space-delineated greatly improved the solutions that were generated.

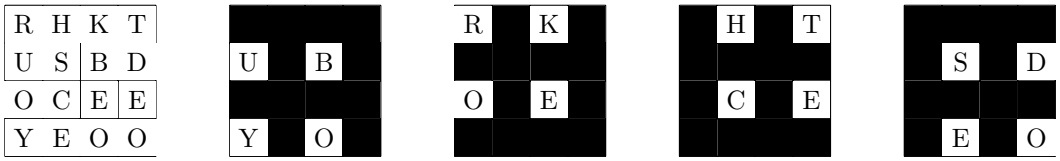
iii. **Find the key and explain how you did it (Hint: it will be a mapping of each character used in the cipher text to a corresponding character in the plain text. i.e. A = M, B = Q, etc.).**

ciphertext	a	b	c	e	g	j	m	n	r	u	v	w	x	y	z
plaintext	l	d	f	c	t	a	n	u	o	y	s	e	r	p	i

This mapping was created using the decrypted plaintext. I simply made a set of the unique characters from the ciphertext and found which characters in the plaintext mapped to the characters in the ciphertext.

3. **Transposition ciphers**

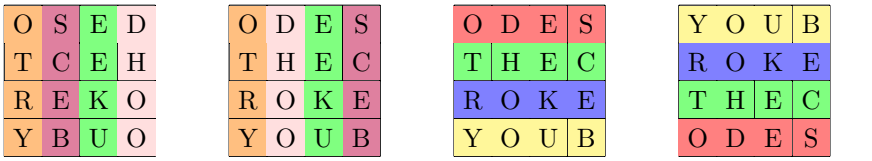
(a) Solve the following Grille cipher using the included cut out. Briefly describe your method of breaking the cipher.



(a) Original grid (b) YOUB (c) ROKE (d) THEC (e) ODES

Overlay the grille over the grid, and rotate it four times. With each rotation, the order of the "decrypted" letters remains the same. The caption for each of the above figures is the plaintext. Altogether, this reads as **YOUBROKETHECODES**.

(b) Solve the following Double Transposition cipher. Briefly describe your method of breaking the cipher.



(a) Original Order (b) Col. 2 ⇔ Col. 4 (c) Reversed rows (d) Final position

I solved this by swapping columns 2 and 4, and then reversing all of the resulting rows. This results in the plaintext **YOUBROKETHECODES**. The final key is (4,3,2,1) and (1,4,3,2).

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 ciphertext KITLKE was generated using a 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"?**

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

Because we have two of the operands of the original XOR equation, we can XOR those two operands to find the original one-time pad key:

```
    111  001  101  010  100  100
⊕   011  010  111  100  011  000
    100  011  010  110  111  100
```

Original one-time pad key: **100 011 010 110 111 100**, or **LKISTL**

(b) **Whats the key if the plain text was "tiller"?**

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

```
    111 010 100 100 000 101
⊕   011 010 111 100 011 000
-----------------------------
    100 000 011 000 011 101
```

Original one-time pad key: **100 000 011 000 011 101**, or **LEKEKR**

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.

   Plaintext: BREAKINGCODESISHARD

6. **BONUS**

   Using any means available, find the plaintext for the following ciphertext and explain briefly but with enough detail to duplicate your method how you solved this:

   MXDXBVTZWVMXNSPBQXLIMSCCSGXSCJXBOVQXCJZMOJZCVCTVWJCZAAXZBCSSCJXBQCJZCOJZ CNSPOXBXSBTVWJCJZDXGXXMOZQMSCSCJXBOVQXCJZMOJZCNSPJZHGXXMOSPLHJZDXZAAXZBX HCSCJXTCSGXSCJXBOVQX

   Plaintext: "NEVER IMAGINE YOURSELF NOT TO BE OTHERWISE THAN WHAT IT MIGHT APPEAR TO OTHERS THAT WHAT YOU WERE OR MIGHT HAVE BEEN WAS NOT OTHERWISE THAN WHAT YOU HAD BEEN WOULD HAVE APPEARED TO THEM TO BE OTHERWISE"

   Again, using https://quipqiup.com, this is decrypted rather quickly. On this website, it is as simple as pasting in raw ciphertext, clicking "Solve" and letting the website do it's job. It's remarkably quick and accurate.