Homework Assignment 1: CIS4362.01 Due 9/15/19

Brandon Thompson 5517

September 9, 2019

1. The earliest known, and simples, use of a substitution cipher was by Julius Caesar. The Caesar cipher involves replacing each letter of the alphabet with the letter standing 3 places further down the alphabet.

   Shift by 3 ('A' mapped to 'D')

   (a) Plain: DORIAN STRUCK THE NORTHERN BAHAMAS AS A CATEGORY FIVE HURRICANE

   Cipher: GRULDQ VWUXFN WKH QRUWKHUQ EDKDPDV DV D FDWHJRUB ILYH KXUULFDQH

   (b) If it is known that a given cipher text is following Caesar cipher but with a different shift, what is the easiest cryptanalysis solution to decrypt the message?

   Can test the first couple of words for every possible shift until a correct output is given. Once the correct shift pattern is known, decrypt the rest of the message.

2. Given the below cipher text which has been encrypted using substitution cipher, answer the following questions.

   UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
   VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
   EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ

   (a) Determine the frequency of letters **P, Z, S, W** in the above cipher text.

   P = 13.33%
   Z = 11.67%
   S = 8.33%
   W = 3.33%

   (b) Find the equivalent plain text letters for **P, Z, S, W** based on their frequency.

   P = E
   Z = T
   S = A
   W = H

3. Briefly explain what a brute-force attack is.

   A brute-force attack is where the attacker tries every possible key on the cipher text until the plain text is revealed.

4. Briefly define the Playfair cipher

   The Playfair cipher is a multiple-letter encryption technique that uses a 5 by 5 matrix of non-repeating letters. Depending on how the plain text letter pairs are related on the matrix determines their cipher text equivalent.

5. Using this Playfair matrix:

M	F	H	I/J	K
U	N	O	P	Q
Z	V	W	X	Y
E	L	A	R	G
D	S	T	B	C

   Encrypt the message: MUST SEE YOU OVER CADOGAN WEST. COMING AT ONCE.

   Cipher text: UZTBDLGZPNNWLGTGTUEROVLDBDUHFPERHWQSRZ

6. Briefly explain a transition cipher.

   A transition cipher performs some sort of permutation on the plain text. This does not map a plain text letter to a cipher text letter, it just scrambles the message. Transposition ciphers can have multiple stages of transposition, making them more difficult the more stages there are.

7. Briefly explain steganography.

   Steganography conceals the existence of a message my hiding the message within other, less meaningful text. Can be done by somehow marking the appropriate letters of the hidden message so the receiver can identify them.

8. Alice and Bob are trying to securely communicate using a Vigenere Cipher technique with the same key. Given the key below answer the following questions.

   Key: DORIAN

   (a) Decrypt the following message that Alice has sent to Bob.

   Cipher text: WVV KRHFWRT PERPCMM VVB'K KRRDHZVG AHK AWBF. WVV KRHFWRT PERPCMM VV QIMAGLBX VEJ MCSA TUDH YCMNQG GMRSRFD JEGWSI BHNQ OCOOELHYUS.
   Plain text: THE CRUCIAL PROBLEM ISN'T CREATING JOBS. THE CRUCIAL PROBLEM IS CREATING JOBS THAT HUMANS PERFORM BETTER THAN ALGORITHMS

   (b) Encrypt the following message on behalf of Bob.

   Plain text: ITSTOOLATE
   Cipher text: LHJBOBOOKM

9. Suppose that the universe is defined as follows:

$$U = \{0,1\}^5 \tag{1}$$

If the weight of all elements of this universe is uniformly distributed, calculate the probability of A which is a subset of U, and A is defined as follows:

$$A = \{\text{all x} \in \text{U s.t. } lsb_2(x) = 11\} \subseteq \text{U} \tag{2}$$

A is every fourth element of U. U has 32 total elements: $\frac{32}{4} = 8$, thus there are 8 elements in A.
Uniform distribution is given as:

$$\forall\ x \in U,\ P(x) = \frac{1}{|U|} \tag{3}$$

Therefor the probability of A is $\frac{8}{32} = \frac{1}{4}$ or 0.25.