Arnel Jerome Adviento - 10130641
Introduction to Cryptography   CPSC 418   Fall 2016
Department of Computer Science
University of Calgary

October 2, 2016

HOME WORK #[NUMBER]

Problem	Marks
1	
2	
3	
4	
5	
6	
7	
Total	

Problem 1. (A substitution cipher cryptanalysis, 10 marks plus 1 bonus mark)

(a) Letter Frequency:

A: 45   B: 2   C: 46   D: 19   E: 26   F: 30   G: 13
H: 4   I: 55   J: 71   K: 28   L: 18   M: 7   N: 30
O: 84   P: 56   Q: 16   R: 58   S: 15   T: 56   U: 56
V: 8   W: 1   X: 135 Y: 2   Z: 23

(b) Plain Text:
Case was twenty-four. At twenty-two, he'd been a cowboy, a rustler, one of the best in the Sprawl. He'd been trained by the best, by McCoy Pauley and Bobby Quine, legends in the biz. He'd operated on an almost permanent adrenaline high, a byproduct of youth and proficiency, jacked into a custom cyberspace deck hat projected his disembodied consciousness into the consensual hallucination that was the matrix. A thief, he'd worked for other, wealthier thieves, employers who provided the exotic software required to penetrate the bright walls of corporate systems, opening windows into rich fields of data.

He's made the classic mistake, the one he's sworn he'd never make. He stole from his employers. He kept something for himself and tried to move it through a fence in Amsterdam. He still wasn't sure how he'd been discovered, not that it mattered now. He'd expected to die, then but they only smiled. Of course he was welcome, they told him, welcome to the money. And he was going to need it. Because–still smiling–they were going to make sure he never worked again.

They damaged his nervous system with a wartime Russian mycotoxin.

(c) William Gibson

$\longrightarrow \mathcal{A}$nswer

Problem 2. (Superencipherment for substitution ciphers, 12 marks)

(a) (i) Let $E_k(M) = M + K (mod\ 26)$ be the shift cipher and M represents the plain text and K the key to shift each letters by.
Let there be keys K_1 and K_2.

We use K_1 to encrypt M in a shift cipher $E_{k1}(M) = M + K_{k1}(mod\ 26)$
Then we apply another shift cipher of key K_2 on $E_{k1}(M)$ resulting in $E_{k2}(E_{k1}(M)) = (M + K_1(mod\ 26)) + K_2(mod\ 26)$
We can simplify it to $M + ((K_1 + K_2)(mod\ 26))$
Where we let $(K_1 + K_2)$ be another key K_3.
Therefore we proved that doing the shift cipher twice just results in another shift cipher with a key of $(K_1 + K_2)$.

(ii) Let $E_k(M) = M + K(mod\ 26)$ be the shift cipher and M represents the plain text and K the key to shift each letters by.

(b) (i) hello
    (ii) there

Problem 3. (Equiprobability maximizes entropy for two outcomes, 12 marks)

(a) Let $p(X_1) = \frac{1}{4}$ and let $p(X_2) = \frac{3}{4}$
$H(X) = -p\ log_2(p) - (1-p)\ log_2(1-p)$
$H(X) = -\frac{1}{4}\ log_2(\frac{1}{4}) - \frac{3}{4}\ log_2(\frac{3}{4})$
$H(X) = 0.5 + 0.311278...$
$H(X) = 0.811278..$

(b) Prove that if $H(X)$ is maximal, then both outcomes are equally likely.
Let $H(X) = -p\log_2(p) - (1-p)\log_2(1-p)$, where p is the probability outcome such that $p + (1-p) = 1$.
Case 1: $p > (1-p)$
Case 2: $p < (1-p)$
Case 3: $p == (1-p)$
Wrong use notes and get derivative to find the maximum

(c) The maximal value of $H(X)$ is 1, when $p(X_1) = \frac{1}{2}$ and $p(X_2) = \frac{1}{2}$

Problem 4. (Key size versus password size, 21 marks)

(a) There are 128 possible characters in the ASCII encoding, and we have a space of 8 characters, therefore that gives us $\mathbf{127^8 = 6.767523424101888110^{16}}$

(b) (i) Since there are, **94** allowed ASCII characters and the ength of the password is exactly **8**. That means at each character slot there are **94** differently possibilities.
Therefore we get the equation:
total permissible passwords = $\mathbf{94^8}$
total permissible passwords = **6095689385410816**
total permissible passwords = $\mathbf{6.1 \times 10^{15}}$

(ii) $\frac{\mathbf{94^8}}{\mathbf{127^8}} = \mathbf{0.09...}$
roughly about 9% of all ASCII is usable for passwords

(c) entropy $= -\sum_0^{\mathbf{94^8}} \left(\frac{1}{\mathbf{94^8}}\right) \mathbf{\log_2}\left(\frac{1}{\mathbf{94^8}}\right)$

(d) entropy $= -\sum_0^{\mathbf{26^8}} \left(\frac{1}{\mathbf{26^8}}\right) \mathbf{\log_2}\left(\frac{1}{\mathbf{26^8}}\right)$

(e) (i)

$$\mathbf{94^x = 2^{128}}$$
$$\mathbf{\ln(94^x) = ln(2^{128})}$$
$$\mathbf{x\, ln(94) = 128\, ln(2)}$$
$$\mathbf{x = \frac{128\, ln(2)}{ln(94)}}$$
$$\mathbf{x = 19.5283034}$$
$$\mathbf{x \approx 20}$$

We need about a 20 characted length password to get an entropy of 128 given 94 usable characters

(ii)

$$\mathbf{26^x = 2^{128}\, \ln(26^x)} \qquad\qquad \mathbf{= ln(2^{128})}$$
$$\mathbf{x\, ln(26) = 128\, ln(2)}$$
$$\mathbf{x = \frac{128\, ln(2)}{ln(26)}}$$
$$\mathbf{x = 27.2314948}$$
$$\mathbf{x \approx 28}$$

We need about a 28 characted length password to get an entropy of 128 given 26 usable characters

$\longrightarrow \mathcal{A}$nswer

Submitted by Arnel Jerome Adviento - 10130641 on October 2, 2016.