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

September 28, 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

⟶ Answer

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

(a) (i) let $\boldsymbol{E_k(M) = M + K(mod\ 26)}$ be the shift cipher and $\boldsymbol{M}$ represents the plain text and $\boldsymbol{K}$ the key to shift each letters by.
Let there be keys $\boldsymbol{K_1}$ and $\boldsymbol{K_2}$.
Then when we use $\boldsymbol{K_1}$ we have $\boldsymbol{E_{k1}(M) = M + K_{k1}(mod\ 26)}$
Then when we apply it to $\boldsymbol{K_2}$ we have $\boldsymbol{E_{k2}(E_{k1}(M)) = (M + K_1(mod\ 26)) + K_{k2}(mod\ 26)}$
We can simplify it to $\boldsymbol{M + ((K_1 + K_2)(mod\ 26))}$
Where we let $\boldsymbol{(K_1 + K_2)}$ be another key $\boldsymbol{K_3}$.
Therefore we proved that doing the shift cipher twice just results in another shift cipher with a key of $\boldsymbol{(K_1 + K_2)}$.

(ii) there

(b) (i) hello

(ii) there

$\longrightarrow$ $\mathcal{A}$nswer

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

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

(b) Prove that if $\boldsymbol{H(X)}$ is maximal, then both outcomes are equally likely.
Let $\boldsymbol{H(X) = -p\log_2(p) - (1-p)\log_2(1-p)}$, where $\boldsymbol{p}$ is the probability outcome such that $\boldsymbol{p + (1-p) = 1}$.
Case 1: $\boldsymbol{p > (1-p)}$
Case 2: $\boldsymbol{p < (1-p)}$
Case 3: $\boldsymbol{p == (1-p)}$

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

$\longrightarrow$ $\mathcal{A}$nswer

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

(a) $\mathbf{127^8}$??

(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 = **6.1** x $\mathbf{10^{15}}$

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

(c) entropy = $-\sum_{0}^{94}(\frac{1}{94})\log_2(\frac{1}{94})$

(d) entropy = $-\sum_{0}^{26}(\frac{1}{26})\log_2(\frac{1}{26})$

(e) (i) hello

(ii) there

$\longrightarrow$ $\mathcal{A}$nswer

Submitted by Arnel Jerome Adviento - 10130641 on September 28, 2016.