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

October 3, 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

$\longrightarrow$ 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 $\boldsymbol{K_2}$.

We use $\boldsymbol{K_1}$ to encrypt $\boldsymbol{M}$ in a shift cipher $\boldsymbol{E_{k1}(M) = M + K_{k1} (mod\ 26)}$
Then we apply another shift cipher of key $\boldsymbol{K_2}$ on $\boldsymbol{E_{k1}(M)}$ resulting in $\boldsymbol{E_{k2}(E_{k1}(M)) = (M + K_1 (mod\ 26)) + K_2 (mod\ 26)}$
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) Let $\boldsymbol{E_k(M) = M + K (mod\ 26)}$ be the shift cipher and $\boldsymbol{M}$ represents the plain text and $\boldsymbol{K}$ represent the key to shift each letters by.

base case (K = 0):

$$\boldsymbol{E_{k0}(M) = M + K_0 (mod\ 26)}$$
$$\boldsymbol{E_{k0}(M) = M + 0}$$

since the key is 0 the plain text remains the same since no shift occurs?
Inductive Step: Assume there is a K, greater than or equal to zero, such that $\boldsymbol{E_k(M) = M + K (mod\ 26)}$.

The key of multiple encipherment is just the sum of all the keys used.

(b) (i) yes, the new keyword of using the keyword $\boldsymbol{WORD}$ and $\boldsymbol{CIPHER}$ is $\boldsymbol{YWGKAFTLLVVU}$
This key is created by adding each corresponding letter of the two keywords based on their index and repeating each keyword if necessary until both keywords are an equal length.

W O R D W O R D W O R D
C I P H E R C I P H E R

Y W G K A F T L L V V U

(ii) Yes, to obtain the corresponding key word you add each letter of $\boldsymbol{m_1}$ to each corresponding character to $\boldsymbol{m_2}$ based on its index in the alphabet $\boldsymbol{(0...25)}$ and modulo it by 26.
eg: $\boldsymbol{m_1.charAt(0) = T}$ and $\boldsymbol{m_2.charAt(0) = I}$. Since $\boldsymbol{I}$ is at index **9** we shift that many letters from $\boldsymbol{T}$ and since we modulo it by 26 the combined vigenere cipher of characters $\boldsymbol{T}$ and $\boldsymbol{I}$ is $\boldsymbol{B}$. As for the length of the new key word, it will be the least common multiple length that $\boldsymbol{m_1}$ and $\boldsymbol{m_2}$ share

⟶ Answer

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) To prove that $\boldsymbol{H(X)}$ is maximal, when both outcomes are equally likely.
we take the derivative of $\boldsymbol{H(X) = -p \log_2(p) - (1-p) \log_2(1-p)}$, where $\boldsymbol{p}$ is the probability outcome such that $\boldsymbol{p + (1-p) = 1}$.

$$
\begin{aligned}
\boldsymbol{H(X)} &= \boldsymbol{-p\log_2(p) - (1-p)\log_2(1-p)} \\
\boldsymbol{H'(X)} &= \boldsymbol{[-\log_2(p) + p\frac{1}{p\ln(2)}] - [(-1)log_2(1-p) + (1-p)\frac{1}{(1-p)\ln(2)}]} \\
\boldsymbol{H'(X)} &= \boldsymbol{-\log_2(p) - \frac{1}{\ln(2)} + log_2(1-p) + \frac{1}{\ln(2)}} \\
\boldsymbol{H'(X)} &= \boldsymbol{-\log_2(p) + log_2(1-p)} \\
\boldsymbol{H'(X)} &= \boldsymbol{log_2(1-p) - \log_2(p)}
\end{aligned}
$$

Now we set H'(X) = 0 and solve for $\boldsymbol{p}$ to find the maximum value for H(X)

$$
\begin{aligned}
\boldsymbol{H'(X)} &= \boldsymbol{log_2(1-p) - \log_2(p)} \\
\boldsymbol{0} &= \boldsymbol{log_2(1-p) - \log_2(p)} \\
\boldsymbol{0} &= \boldsymbol{(1-p) - p} \\
\boldsymbol{p} &= \boldsymbol{1-p} \\
\boldsymbol{2p} &= \boldsymbol{1} \\
\boldsymbol{p} &= \boldsymbol{\frac{1}{2}}
\end{aligned}
$$

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

$\longrightarrow$ Answer

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 $\mathbf{127^8 = 6.7675234241018881 10^{16}}$

(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 = **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 = $-\sum_{\mathbf{0}}^{\mathbf{94^8}} (\frac{\mathbf{1}}{\mathbf{94^8}}) \log_{\mathbf{2}}(\frac{\mathbf{1}}{\mathbf{94^8}})$

(d) entropy = $-\sum_{\mathbf{0}}^{\mathbf{26^8}} (\frac{\mathbf{1}}{\mathbf{26^8}}) \log_{\mathbf{2}}(\frac{\mathbf{1}}{\mathbf{26^8}})$

(e) (i)

$$\begin{aligned} \mathbf{94}^{\boldsymbol{x}} &= \mathbf{2}^{\mathbf{128}} \\ \ln(\mathbf{94}^{\boldsymbol{x}}) &= \boldsymbol{ln}(\mathbf{2}^{\mathbf{128}}) \\ \boldsymbol{x}\, \boldsymbol{ln}(\mathbf{94}) &= \mathbf{128}\, \boldsymbol{ln}(\mathbf{2}) \\ \boldsymbol{x} &= \frac{\mathbf{128}\, \boldsymbol{ln}(\mathbf{2})}{\boldsymbol{ln}(\mathbf{94})} \\ \boldsymbol{x} &= \mathbf{19.5283034} \\ \boldsymbol{x} &\approx \mathbf{20} \end{aligned}$$

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

(ii)

$$\begin{aligned} \mathbf{26}^{\boldsymbol{x}} &= \mathbf{2}^{\mathbf{128}} \ln(\mathbf{26}^{\boldsymbol{x}}) && = \boldsymbol{ln}(\mathbf{2}^{\mathbf{128}}) \\ \boldsymbol{x}\, \boldsymbol{ln}(\mathbf{26}) &= \mathbf{128}\, \boldsymbol{ln}(\mathbf{2}) \\ \boldsymbol{x} &= \frac{\mathbf{128}\, \boldsymbol{ln}(\mathbf{2})}{\boldsymbol{ln}(\mathbf{26})} \\ \boldsymbol{x} &= \mathbf{27.2314948} \\ \boldsymbol{x} &\approx \mathbf{28} \end{aligned}$$

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

⟶ Answer

Submitted by Arnel Jerome Adviento - 10130641 on October 3, 2016.