CPSC 418 / MATH 318 — Introduction to Cryptography
ASSIGNMENT 1

Name: Hanum Lee
Student ID: 30010205

Problem 1 — Superencipherment for substitution ciphers, 12 marks

(a) i. Single Cipher: $E_k(M) \equiv M + K \pmod{26}$
Double Cipher:

$$\begin{aligned} E_{K_1}(E_{K_2}(M)) &\equiv E_{K_1}(M + K_2 \pmod{26}) \\ &= M + K_2 \pmod{26} + K_1 \pmod{26} \\ &= M + K_3 \pmod{26} \end{aligned}$$

for $K_{1,2,3} \in Keyspace$

ii. Assume: $E_k(m) \equiv m + k \pmod{26}$ For all $m \in \mathcal{M} \& k \in \mathcal{K}$
Base case: $E_{K_1}(E_{K_2}(M)) \equiv M + K_3 \pmod{26}$ (Proven at 1.(a).i)
Inductive Hypothesis: $E_{k_n}(E_{k_{n-1}}...E_{k_1}(m)) \equiv m + (k_{n+n-1+...+1}) \pmod{26}$ is true for $n > 2$
Inductive Step:
Want to show that: $E_{k_{n+1}}(E_{k_n}...E_{k_1}(m)) \equiv m + k_{(n+1)+n+..+1} \pmod{26}$
$E_{k_{n+1}}(E_{k_n}...E_{k_1}(m)) = E_{k_{k+1}}(m + k_{n+...+1} \pmod{26})$ (with Inductive Hypothesis)

$$\equiv m + k_{(n+1)+n+..+1} \pmod{26}$$

where $k_{(n+1)+n+...+1} = k_q$ for $q \in \mathbb{Z}$
Therefore, the induction holds true.

(b) The length of new keyword w is least common multiple of the length two words m and n. Since Vigenere Cipher is a shift cipher to each character with the key as the characters in key word, $V_{k_1}(V_{k_2}(m)) = V_{k_1+k_2}(M)$. To find the new keyword w, use the shorter word between w_1 and w_2 as key for the other one and apply Vigenere Cipher to it.

Problem 2 — Key size versus password size, 21 marks]

(a) $2^7 * 2^7 * 2^7 * 2^7 * 2^7 * 2^7 * 2^7 2^7 = 2^{7*8} = 2^{56}$

(b) i. $98 * 98 * 98 * 98 * 98 * 98 * 98 * 98 = 98^8$

ii. $\frac{98^8}{2^{56}} * 100 = 11.81\%$

(c) $H(X) = \sum_{i=0}^{n} p(X_i) \log_2 \frac{1}{p(X_i)}$

In this case:

$H(X) = 8 * \sum_{i=1}^{n} \frac{1}{n} \log_2 n$ (Since all characters have equal chance of appearing for each character and there are 8 characters in passwords)

$= 8 * \log_2 94$

$= 52.43$

(d) Similar as above

$H(X) = 8 * \sum_{i=1}^{n} \frac{1}{n} \log_2 n$

$= 8 * \log_2 26$

$= 37.60$

(e) i. $128 = l * \log_2 94$ where l is length of the password

$l = \frac{128}{\log_2 94}$

$l = 19.35$

So, at least 20 characters

ii. $128 = l * \log_2 26$ where l is length of the password

$l = \frac{128}{\log_2 26}$

$l = 27.23$

So, at least 28 characters

Problem 3 — Equiprobability maximizes entropy for two outcomes, 12 marks

(a) $H(X) = p(X_1)\log_2(\frac{1}{p(X_1)}) + p(X_2)\log_2(\frac{1}{p(X_2)})$
$= \frac{1}{4}\log_2 4 + \frac{3}{4}\log_2\frac{4}{3}$
$= \frac{1}{2} + 0.311$
$= 0.81$

(b) To find maximum of a function, first, we need to find derivative of the function.
$\frac{d}{dp} - p\log_2(p) - (1-p)log_2(1-p)$
$= \frac{d}{dp}(-p\frac{\log p}{\log 2} - (1-p)\frac{\log(1-p)}{\log 2})$ (Using product law and identity)
$= -(\frac{p}{p} + \frac{\log p}{\log 2}) - (\frac{(1-p)}{(1-p)} + \frac{\log(1-p)}{\log 2})$
$= -1 - \frac{\log p}{\log 2} + 1 + \frac{\log(1-p)}{\log 2}$
$= \frac{\log(1-p) - \log(p)}{\log 2}$
Then we find the p value when the equation above is equal to 0 which is $p = \frac{1}{2}$, therefore, it shows that entropy is maximal when both outcomes are equally likely.

(c) Since we know the value p, we just substitute it to the equation given.
$H(X) = \frac{1}{2}\log_2(2) + (\frac{1}{2})\log_2(2) = 1$
So maximal value of $H(X)$ is 1.

Problem 4 — Conditional entropy, 12 marks

(a) To find $H(M|C)$, I have to compute:
$\sum_{i=1}^{4} p(C_i) \sum_{j=1}^{4} p(C_i|M_j) \log_2(\frac{1}{p(C_i|M_j)})$
For $p(C_1)$, $\sum_{j=1}^{4} p(C_1|M_j) \log_2(\frac{1}{p(C_1|M_j)}) = \frac{1}{2}\log_2 2 + \frac{1}{2}\log_2 2 + 0 + 0 = 1$ Assuming that M_1 and M_2 has equal chance of appearing when cipher text is C_1
Repeat this for $p(C_2), p(C_3), p(C_4)$
For $p(C_2)$, $\sum_{j=2}^{4} p(C_2|M_j) \log_2(\frac{1}{p(C_2|M_j)}) = 0 + 0 + \frac{1}{2}\log_2 2 + \frac{1}{2}\log_2 2 = 1$
This goes same for $p(C_3), p(C_4)$,
So, $\sum_{i=1}^{4} p(C_i) \sum_{j=1}^{4} p(C_i|M_j) \log_2(\frac{1}{p(C_i|M_j)}) = 4$

(b) If cryptosystem is providing perfect secrecy implies that knowing the ciphertext $\mathcal{C}$ gives no information about $\mathcal{M}$.Which could also means that knowing message does not give information about ciphertext. This can be represented as $H(\mathcal{C}|\mathcal{M}) = H(\mathcal{C})$.
Then, $H(C|M) = \frac{p(C)p(M|C)}{p(M)}$
For $H(\mathcal{C}|\mathcal{M}) = H(\mathcal{C})$ to hold true, $H(\mathcal{M}|\mathcal{C}) = H(\mathcal{M})$ has to hold true.
Therefore, for cryptosystem to have perfect secrecy, $H(\mathcal{M}|\mathcal{C}) = H(\mathcal{M})$ has to hold true.

(c) No, With the methods used above, we can find $H(C|M)$ and $H(C)$

$$H(C|M) = \sum_{i=1}^{4} p(M_i) \sum_{j=1}^{4} p(M_i|C_j) \log_2(\frac{1}{p(M_i|C_j)})$$

Since all of the $M \in \mathcal{M}$ has equal possibility, I just have to compute one of them.
For $p(M_1)$, $\sum_{j=1}^{4} p(M_1|C_j) \log_2(\frac{1}{p(M_1|C_j)}) = \frac{1}{2}\log_2 2 + 0 + 0 + \frac{1}{2}\log_2 2 = 1$
So, $H(C|M) = 4$ and $H(C) = 8$
Since, $H(\mathcal{C}|\mathcal{M}) \neq H(\mathcal{C})$, example does not provide perfect secrecy.