CPSC 418 / MATH 318 — Introduction to Cryptography
ASSIGNMENT 1

Name: test
Student ID: test

Problem 1 — Superencipherment for substitution ciphers, 12 marks

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

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

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

ii. Assume: $E_k(m) \equiv m + k \pmod{26}$ For all $m \in M \& k \in K$
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 $q \in Z$
Therefore, the induction holds true.

(b)

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.

$\frac{d}{dy} - p\log_2(p) - (1-p)log_2(1-p)$

$= -\frac{d}{dy}(p)\frac{\ln p}{\ln 2} - (1-p)\frac{\ln(1-p)}{\ln 2} =$

(c) Find where the value of the derivative above is 0. Then find which point goes from negative to positive.

Problem 4 — Conditional entropy, 12 marks

(a)

(b)

(c)

Problem 5 — Perfect secrecy and joint entropy, 43 marks

***** Remove the text for this problem if you don't attempt it. *****

(a) i.

ii.

iii.

iv.

v.

(b) i.

ii.

iii.

iv.

v.

vi.

vii.

Problem 7 — Mixed Vigenère cipher cryptanalysis, 10 marks

***** Remove the text for this problem if you don't attempt it. *****