Solutions to Assignment 4

Barr 2.4, p. 106 #2

2. The deciphered message is WELL IF I CALLED THE WRONG NUMBER WHY DID YOU ANSWER THE PHONE?

Barr 2.4, p. 106 #4

4. The Enciphered message is
CEHIT OTDRC EESDS TDUMN LESCH LETOI SIOO ENIAE LHMEE RCTWR AVHWP TMSBT DIEOM NTSPI ONESE DHFYO DIUWN STBMY RVINT LII

Barr 2.5, p. 118 #4

4. The original message is BEAUTY IS ONLY THE PROMISE OF HAPPINESS.

Barr 2.5, p. 119 #6

6. (i) is the polyalphabetic substitution; (ii) is the transposition; (iii) is the monoalphabetic substitution.

Barr 2.6, p. 131 #5, #6

5.
(a) There are P(15,10) = 15!/(15-10)! = 15!/5! = 1.089729×10^{10} ways to **arrange** 10 books from 15.
(b) There are P(8,3) = 8!/(8-3)! = 8!/5! = 336 ways to fill the offices.

6.

(a) There are C(15,10) = 15! / (5!10!) = 3003 ways to **choose** 10 books from 15.

(b) There are C(8,4) = 8! / (4!4!) = 70 ways to select a committee of four from 8 people.

Barr 2.6, p. 133 #14*

14.*

n	1	2	…	6	7	8	9	10	11	12
b(n)	0	0.032	…	0.383	0.5023	0.615	0.714	0.797	0.863	0.911

where b(n) is the probability of at least 1 pair of coincident birthdays in a group of n people with birthdays in May. Thus, to be at least 50% certain of at least 1 pair of coincident birthdays, 7 people must be chosen. To be at least 90% certain, 12 people must be selected.

Barr 2.7, p. 141 #2*

2.* The index of coincidence is 0.040 and the estimated keyword length is 19. This differs significantly from the keyword length estimates of 2, 4, or 8 obtained by Kasiski test. However, since this is a fairly large number, it strengthens the hypothesis that the keyword length is 8.

D1. Done in Class.

D2* Use an induction argument to show $F(n)^2 - F(n+1)F(n-1)$ is either 1 or -1 for any natural number n.

Recall $F(1)=1$, $F(2)=1$, $F(n)=F(n-1)+F(n-2)$.

Base Case: let $n=2$. $[F(2)]^2 - F(2+1)F(2-1)$

$= [1]^2 - F(3)F(1)$; $F(3)=F(2)+F(1)=2$

$= 1-(2)(1) = -1$

So, the statement is true for $n=2$.

Next,

Assume the statement holds for n. Show statement holds for $n+1$.

Statements holds for $n \Rightarrow F(n)^2 - F(n+1)F(n-1) = \pm 1$.

What is required to show is $F(n+1)^2 - F(n+2)F(n) = \pm 1$.

$$F(n+1)^2 - F(n+2)F(n) = [F(n)+F(n-1)]^2 - [F(n+1)+F(n)](F(n))$$

$$= F(n)^2 + 2F(n)F(n-1) + F(n-1)^2 - F(n+1)F(n) - F(n)^2$$

Replacing for $F(n+1)$:

$= 2F(n)F(n-1) + F(n-1)^2 - F(n)[F(n)+F(n-1)]$

$= 2F(n)F(n-1) + F(n-1)^2 - F(n)^2 - F(n)F(n-1)$

$= -F(n)^2 + F(n-1)^2 + F(n)F(n-1)$

$= -F(n)^2 + F(n-1)[F(n-1)+F(n)]$, but $F(n-1)+F(n)=F(n+1)$

$= -F(n)^2 + F(n-1)F(n+1)$

$= -[F(n)^2 - F(n+1)F(n-1)]$

By assumption $F(n)^2 - F(n+1)F(n-1)$ is ± 1.

So, $F(n+1)^2 - F(n+2)F(n) = \pm 1$.

Thus, by induction,

$F(n)^2 - F(n+1)F(n-1)$ is either 1 or -1 for any natural number n.