Solutions to Assignment 1

Barr 1.1: 2, 6, 14, 20, 21, 22.

2. Replace A by Z, B by Y and so on.

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Z Y X W V U T S R Q P O N M L K J I H G F E D C B A

Deciphered Message: THIS WHOLE LAND SHALL BECOME A RUIN AND A WASTE.

6.
(a) FRIENDS ROMANS AND COUNTRYMEN, LEND ME YOUR EARS is enciphered as IULHQGV URPDQV FRXQWUBPHQ OHQG PH BRXU HDUV.
(b) EHZDU HWKHL GHVRI PDUFK is deciphered as BEWARE THE IDES OF MARCH.
(c) Using ROT13 encipherment CAN WE EVER HAVE TWO MUCH OF A GOOD THING is enciphered as PNA JR RIRE UNIR GBB ZHPU BS N TBBQ GUVAT.
(d) Shifting each letter 8 letters to the left (or 17 letters to the right),
ZMQVO QAJMB BMZBP IVAMM UQVOB WJM is deciphered as BEING ISBET TERTH ANSEE MINGT OBE. So, the deciphered message is BEING IS BETTER THAN SEEMING TO BE.

14. The message is deciphered as: WELL GOT WEALTH MAY MEET DISASTER, BUT ILL GOT WEALTH DESTROYS ITS MASTER.

20. Using ADFGVX and the keyword BERLIN,
GVGGF XVXXD GGGXD DFVGD XAAVV XFXAX is deciphered as ENEMY RETREATING.
21. The work needed to decipher a Single Shift Encipherment is exactly the same as the work needed to decipher a Double Shifted Encipherment. A shift of 3, followed by a shift of 5 would yield the same encipherment as a shift of 8 (Try it!). Using Trial And Error, KNCFNNW OARNWMB CQNAN RB WX WNNM XO SDBCRLN is deciphered as BETWEEN FRIENDS THERE IS NO NEED OF JUSTICE.

22.
(a) Given Block length b and rotation r. First break the given enciphered message into blocks of size b. Then rotate each letter in the block r places.
(b) Using a block length of 6 and rotation 3, the message is deciphered as THE UNIVERSE IS MADE OF STORIES, NOT ATOMS.
(c) The book has a typo here that most of you caught: The enciphered message should read IVGTH EPEEP LOANE WWERD ONDAH ETTHY NKIHE THAYE AVEWN ACFT, not IVGTH EPEEP LONEA WWERD ONDAH ETTHY NKIHE THAYE AVEWN ACFT. That is, the third group of ciphertext letters should be LOANE, not LONEA.
The most systematic approach would be to first assume a block length of 2 and consider a rotation of 0 and 1. Then assume a block length of 3 and consider a rotation of 0, 1 and 2. Repeat until the message is recovered. Note that the maximum block length will be the length of the message, so it is quite possible to break the cipher.
(d) The amount of work the cryptoanalyst is required to do dramatically increases under the assumption that a succession of 2 rotations with different block lengths and rotation amounts had been used. Note that a systematic approach would now be the following: First assume the 1st rotation involved a block length of 2 and rotation 0. Try all possible block lengths and rotation amounts for the 2nd rotation. Then, repeat this procedure assuming a rotation of 1 for the 1st rotation. Then, increase the block length of the 1st rotation to 2 and assume a rotation of 0. Try all possible block lengths and rotation amounts for the 2nd rotation. Then, repeat this procedure assuming a rotation of 1 for the 1st rotation, and so on. Note the large number of possibilities. Also note that even if the cryptoanalyst guesses correctly the block length and rotation amount of the 1st rotation, he/she still has to go through all possible rotation
block lengths and rotation amounts for the 2nd rotation – never knowing whether their initial guess is right or wrong.

A.1

There are 3 parades of 4 people (4x1, 2x2, 1x4 – Note that 2x2 is only counted ONCE).
There are 2 parades of 5 people (5x1, 1x5).
There are 4 parades of 6 people (1x6, 2x3, 3x2, 6x1).
There are 2 parades of 7 people (1x7, 7x1).
There are 4 parades of 8 people (1x8, 2x4, 4x2, 8x1).
There are 3 parades of 9 people (1x9, 3x3, 9x1).

Some Odd Numbers with exactly four parades are 15, 21, 27, 33, 35, 39, 55.
Note that all the odd numbers are divisible only by primes (and 1 obviously).
In particular, there are 2 kinds of Odd Numbers that yield exactly four parades:

1) An odd number that is the product of 2 distinct primes only. For Example, 15 = 3 \times 5, and 21 = 3 \times 7. Note that 75 = 3*5*5 is also a product of primes but it has 6, rather than 4 parades, so being the product of 2 primes only is important.
Example: 105 = 3 \times 5 \times 7 has 6 parades as well, even though 105 only has prime divisors. Also, note that 9 = 3 \times 3 is also the product of primes but there only 3 parades of 9 people, so the primes have to be distinct.

2) An odd number that is the cube of a prime number. For Example, 27 = 3*3*3, and 125 = 5*5*5, 243 = 7*7*7.