Chapter 3

1) 16 -
For this cipher, instead of trying to satisfy D (C, K_2) = E (P, K) like how Trudy does is for C = E (E (P, K_1), K_2) key. We would instead find K_1 and K_2 that satisfy E (C, K_2) = E (P, K_1). Everything else is the same in the meet-in-the-middle attack. We would still precompute a table of 2^{56} containing E(P,K) and K_1 for all key values of K_1. We will also decrypt C with K_2 until we found a value X = E(C, K_2) from the table instead of X = D(C,K_2) as per the method from the book.

2) 25 –
a.
The decryption rule is: P_0 = D (C_0 XOR IV, K), P_1 = D (C_1 XOR C_0, K), P_2 = D(C_2 XOR C_1, K) …

b. When comparing to CBC mode, this is mode is similar to ECB, which is much less secure than CBC. Tracy can compute C_i XOR C_{i-1} to find what's stored in the ECB data. So, this mode has all the short comings of ECB like knowing the plaintext block will yield the same ciphertext block!

3) 31 –
a.
if CBC mode is used with the same IV then the same plaintext will show the same cipher text however only initially, once the plain text changes, then the cipher text will change from then on as well.
b.
If CTR mode is used, then the same plaintext will show the same cipher text.
c.
CTR mode is much less secure since the same keystream is used each time. CBC is much better since the plaintext shows the cipher initially, but then after each time the plain text changes, the cipher will be different.

Chapter 4

4) 5 –
Because $M^{ed} = M^{de}$ mod N is correct, this essentially shows that the public {} and private [] are analogous in [{M}Alice]Alice = M and {[M]Alice}Alice = M showing that these both work in RSA

5) 20 –
a.
$m^{-1}C$ = 6 * 20 = 120 = 26 mod 47
Super increasing knapsack:
3 5 10 23
It has 23 leaving 3.
No 10 or 5. But it does have 3
It has a 3 and 23 therefore.
1001

b.

$m^{-1}C = 6 * 29 = 174 = 33 \bmod 47$
Super increasing knapsack:
3 5 10 23
It has 23 leaving 10, has 10
Leaving 0, doesn't have 5 or 3
It has a 10 and 23 therefore:
0011

c.
since $6 * m = 1 \bmod 47$
$m = 8$
$3m = 3 * 8 = 24 \bmod 47$
$5m = 5 * 8 = 40 \bmod 47$
$10m = 10 * 8 = 33 \bmod 47$
$23m = 23 * 8 = 43 \bmod 47$

key = (24,40,33,43)

6) 26 –

$g = 1$
$g = p – 1$

a. $g^n = 1 \bmod p$ for all n, if g was equal to one then it would be easy to break the encryption so g is not a generator therefore not an allowable choice
b. $g = -1 \bmod p$, $g^n \bmod p$ is either 1 or -1 for n, so g is not a generator therefore it is not an allowable choice.