6.15

HW7 $e(x_1)\cdot e(x_2) \bmod n = e(x_1 \cdot x_2) \bmod n$

$d(y_1)\cdot d(y_2) \bmod n = d(y_1 \cdot y_2) \bmod n$

$e_{(n,b)}(x_1)\cdot e_{(n,b)}(x_2) \bmod n = \left((x_1)^b \bmod n \cdot (x_2)^b \bmod n\right) \bmod n =$

$= (x_1^b \cdot x_2^b) \bmod n = (x_1 \cdot x_2)^b \bmod n = e_{(n,b)}(x_1 \cdot x_2)$

Chosen ciphertext attack: Oscar chooses some ct + has one time access to decrypt it.

$\hat{x} = d(\hat{y})$, $\hat{x}$ + $\hat{y}$ known.

Bob $e(x) = \boxed{y} \longrightarrow$ Alice

intercept

Oscar

Oscar: pick x_1 and compute $y_1 = e(x_1)$

compute $\hat{y} = (y_1 \cdot y) \bmod n$. $\hat{x} = d(\hat{y}) = d(y_1 \cdot y) = d(y_1)\cdot d(y) = x_1 \;= x$

thus,

$\hat{x} = x_1 \cdot x \bmod n$ (oscar knows $\hat{x}$ & x_1)

$\hat{x} \cdot x_1^{-1} = x$

6.16

a. If Oscar has access to use a chosen ciphertext attack, then it would be beneficial for him to encrypt the whole alphabet, and he could use that to decrypt each letter in Alice's ciphertext.

b. He could factor n to get phi(n), then use b and phi(n) to plug into the egcd algorithm. This would yield our *a*, which we could plug into the square and multiply algorithm along with *n* and the ciphertext to get our message in plaintext numbers. This is not the way the book wants it, but it's the only way I could figure it out.

6.16b.

$\sqrt{200} \rightarrow$ factor(18721)

$97 \cdot 193$

$\phi(n) = (p-1)(q-1)$

$= (96)\,192$

$\phi(n) = 18432 \rightarrow$ egcd$(b, \phi(n))$

egcd(25, 18432)

$\{1 \quad 5161 \quad -7\}$

$5161 \downarrow a$

sam(365, 5161, 18721) → 21 → V

sam(0, 5161, 18721) → 0 → A

4845 → 13 → N

14930 → 8 → I

2608 → 11 → L

VANILLA

6.18

All Oscar would have to do is calculate the inverse of the operation that was performed. He would have to do the cube root of y $\sqrt[3]{y_i}$ and then try a different modulus until he finds a message that makes sense.