<u>Solutions to Assignment 6</u>

Barr 3.2, Page 200: 2, 3, 4.

2.

(a) 10110 $\oplus$ 01011 = 11101

(b) 101011 $\oplus$ 101011 = 000000

(c) 010010 $\oplus$ 010010 = 000000

3. If $y_1 y_2 y_3 y_4 = x_3 x_2 x_4 x_1$, then $x_1 x_2 x_3 x_4 = y_4 y_2 y_1 y_3$. So, $f^{-1}(y_1 y_2 y_3 y_4) = y_4 y_2 y_1 y_3$.

4. D is the inverse of E in the x variable. To find it, let $y_1y_2 = x_2x_1 \oplus k_1k_2$. Then $x_1 + k_2 \equiv y_2 \pmod 2$ and $x_2 + k_1 \equiv y_1 \pmod 2$. So $x_1 \equiv y_2 + k_2 \pmod 2$ and $x_2 \equiv y_1 + k_1$ (mod 2). This means $x_1x_2 = y_2y_1 \oplus k_2k_1$. So $D(y_1y_2, k_1k_2) = y_2y_1 \oplus k_2k_1$ satisfies the desired identity: with $y_1y_2 = E(x_1x_2, k_1k_2) = x_2x_1 \oplus k_1k_2$, we get

$$\begin{aligned} D(E(x, k), k) &= y_2y_1 \oplus k_2k_1 \\ &= (x_1x_2 \oplus k_2k_1) \oplus k_2k_1 \\ &= x_1x_2 = x. \end{aligned}$$

F1.

f(0121012101) = 1(0) + 2(1) + 3(2) + … + 9(0) = 10(1) = 50 (mod 11) = 6.

Plugging an ISBN into f should give you a remainder of 0.

F2.

(a) d = 4:

Program 1 takes 2368 seconds.

Program 2 takes 0.05 seconds.

Program 3 takes 15,000 seconds.

Thus, Program 2 is faster than Program 1 which is faster than Program 3.

(b) d = 100:

Program 1 takes 37 x 10^6 seconds.

Program 2 takes 5 x 10^{94} seconds.

Program 3 takes 1.5 x 10^{12} seconds.

Thus, Program 1 is faster than Program 3 which is faster than program 2.

F3.

If d = 20, E will take (at most) 0.01082 seconds.

If d = 22, E will take (at most) 0.01309 seconds.

If d = 40, E will take (at most) 0.04324 seconds.

If d = 20, F will take (at most) 10 seconds.

If d = 22, F will take (at most) 100 seconds.

If d = 40, F will take (at most) 1 x 10^{11} seconds.

F4.

To try all possible 56 bit keys, D will take $2^{56} / 2^{38} = 2^{18}$ = 262, 144 seconds.

To try all possible 64 bit keys, D will take $2^{64} / 2^{38} = 2^{26}$ = 67,108,864 seconds.

To try all possible 128 bit keys, D will take $2^{128} / 2^{38} = 2^{74}$ = 1.89 x 10^{22} seconds.

F5. The Complexity of Programs 1, 2, 3, D, E, F.

Polynomials $O(d^r)$ for some r	Program 1				Program E	
Exponential $O(r^d)$ for some r		Program 2		Program D		Program F
Something bigger than any polynomial but smaller than any exponential			Program 3			
Something bigger than any exponential						