Andrew Johnson

CS427

HW3

Problem 1)

Define a two round cipher to look like

```
$\underline{F^*(\{k_1,k_2\},(L,R))}$
$L' \leftarrow R$
$R' \leftarrow L \oplus f(k_1,R)$
$L'' \leftarrow R'$
$R'' \leftarrow L' \oplus f(k_2,R')$
```

If we have two messages M_1 and M_2, with their right sides being the same. ($M_1 = L_1R$ and $M_2 = L_2R$)

Then when we send them through F*, the two left sides of the cipher texts will be xor'd with the same thing.

```
$\underline{Adv(M_1,M_2)}$
$X = F^*(M_1)$     $//M_1 = L_1R$
$Y = F^*(M_2)$     $//M_2 = L_2R$
If($X_{left} \oplus Y_{left} == L_1 \oplus L_2$)
   Return True
Else
   Return False
```

If the adversary returns true, you know you are in the real library. If it proves false, you are highly likely in the random library.

Problem 2)

a)

```
$\underline{Dec(k, c_0 \ldots c_L)}$
$m_0 = c_0$
for i = 1,…,L:
   $m_i = F^{-1}(k, c_i \oplus m_{i-1})$
return $m_1,\ldots,m_L$
```

b)

```
$Adv(M=\{m_1,\ldots,m_L\})$
   C = Challenge(M)
   $X = c_0 \oplus c_1$      // $F(k,m_1)$
   T = Challenge($\{m_1,m_3,m_5\}$)
   $Y = t_0 \oplus t_1$      // $F(k,m_1)$
   If(X == Y)
      Return True
   Return False
```

Problem 3)

Let's have L-1 m's that are blen bits, and let out m_L be blen – 1 bits. We will send multiple sets of M with m_L as the last block sent in. There should be about a one half chance that two c_L's from different Challenge calls will be matching if we are in the real library. If we are in the Rand library it would be about ($1/2^{blen}$).

```
$\underline{Adv(M=\{m_1,m_2,\ldots,m_L\}}$
   A = Challenge($m_1,m_i,..,m_j,m_L$)
   B = Challenge($m_1,m_k,..,m_n,m_L$)
    :
   Z = Challenge($m_1,m_o,..,m_p,m_L$)
   If ($a_L$ == ($b_L$ or $c_L$ or … or $z_L$))
      Return true
   Return False
```

Problem 4)

(a)

```
CPA$_new
k←{0,1}^λ
S←{}      //Empty Set
Enc(r,m)
    If(r∈S)
        return null
    S = S U {r}
    x = F(k,r) ⊕ m
    return (r,x)
```

(b)

```
Adv(P)
    R ← {0,1}^λ    //Our 1st chosen IV
    X = Challenge(R,P)
    S ← {0,1}^λ    //2nd chosen IV
    P' = $S \oplus R \oplus P$
    Y = Challenge(S,P')
    If(X == Y)
        Return True
    Return False
```

Since we can choose our IV's then once we pass in the first IV and plaintext, we can XOR the first IV with our plaintext (to simulate the beginning of the first challenge) and XOR that with our second chosen IV. So when the entire XORed string is passed in the challenge, it should replicate the first challenge. Thus if both outputs are the same, you know you are in the real library.