Andrew Johnson

CS427

|  |
| --- |
| F\*({k1,k2},(L,R)) |
| L’ ← R |
| R’ ← Lf(k1,R) |
| L’’ ← R’ |
| R’’ ← L’ f(k2,R’) |

HW3

Problem 1)

Define a two round cipher to look like

If we have two messages M1 and M2, with their right sides being the same. (M1 = L1R and M2 = L2R)

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

|  |
| --- |
| Adv(M1,M2) |
| X = F\*(M1) //M1 = L1R |
| Y = F\*(M2) //M2 = L2R |
| If(Xleft  Yleft == L1 ­ L2) |
| Return True |
| Else  Return False |

|  |
| --- |
| Dec(k, c0…cL) |
| m0 = c0 |
| for i = 1,…,L: |
| mi = F-1(k, ci mi-1) |
| return m1,…,mL |

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)

|  |
| --- |
| Adv(M={m1,…,mL}) |
| C = Challenge(M) |
| X = c0 c1 // F(k,m1) |
| T = Challenge({m1,m3,m5}) |
| Y = t0 t1 // F(k,m1) |
| If(X == Y) |
| Return True |
| Return False |

b)

Problem 3)

|  |
| --- |
| Adv(M={m1,m2,…,mL} |
| A = Challenge(m1,mi,..,mj,mL) |
| B = Challenge(m1,mk,..,mn,mL) |
| :  Z = Challenge(m1,mo,..,mp,mL) |
| If (aL == (bL or cL or … or zL)) |
| Return true |
| Return False |

Let’s have L-1 m’s that are blen bits, and let out mL be blen – 1 bits. We will send multiple sets of M with mL as the last block sent in. There should be about a one half chance that two cL’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 (1/2blen).

|  |
| --- |
| CPA$new |
| k←{0,1}λ |
| S←{} //Empty Set |
| Enc(r,m) |
| If() |
| return null |
| S = S U {r} |
| x = F(k,r) m |
| return (r,x) |

Problem 4)

(a)

|  |
| --- |
| Adv(P) |
| R ← {0,1}λ //Our 1st chosen IV |
| X = Challenge(R,P) |
| S ← {0,1}λ //2nd chosen IV |
| P’ = |
| Y = Challenge(S,P’) |
| If(X == Y)  Return True |
| Return False |

(b)

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.