Intro to Crypto Assignment 3

Jan Hendron(s1049777), Nick Weibe(s4163168)

September 2021

Question 1

(a)

$$\begin{aligned} C_L &= (P_L \oplus F(P_R, K_1)) \oplus F((P_R \oplus F((P_L \oplus F(P_R, K_1)), K_2)), K_3 \\ C_R &= P_R \oplus F((P_L \oplus F(P_R, K_1)), K_2) \end{aligned}$$

(b)

$$\begin{aligned} P_L &= (C_L \oplus F(C_R, K_3) \oplus F((F(C_L \oplus F(C_R, K_3), K_2) \oplus C_R), K_1) \\ P_R &= C_R \oplus F((C_L \oplus F(C_R, K_3)), K_2) \end{aligned}$$

(c)

$$\begin{aligned} a &= (0 \oplus F(0, K_3) \oplus F((F(0 \oplus F(0, K_3), K_2) \oplus 0), K_1) \\ &= F(0, K_3) \oplus F((F(F(0, K_3), K_2)), K_1) \end{aligned}$$

$$\begin{aligned} b &= 0 \oplus F((0 \oplus F(0, K_3)), K_2) \\ &= F(F(0, K_3), K_2) \end{aligned}$$

(d)

$$\begin{aligned} c &= (0 \oplus F(b, K_1)) \oplus F(b \oplus F(0 \oplus F(b, K_1), K_2), K_3) \\ &= F(b, K_1) \oplus F(b \oplus (F(F(b, K_1), K_2), K_3) \end{aligned}$$

$$\begin{aligned} d &= b \oplus F((0 \oplus F(b, K_1)), K_2) \\ &= b \oplus F(F(b, K_1), K_2) \end{aligned}$$

(e)

$$\begin{aligned} e &= ((a \oplus c) \oplus F(d, K_3) \oplus F((F((a \oplus c) \oplus F(d, K_3), K_2) \oplus d), K_1) \\ f &= d \oplus F(((a \oplus c) \oplus F(d, K_3)), K_2) \end{aligned}$$

(f) First, we find the value of $a \oplus c$

$$\begin{aligned} &F(0, K_3) \oplus F(F(F(0, K_3), K_2), K_1) \\ &\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \oplus \\ &F(b, K_1) \oplus F(b \oplus (F(F(b, K_1), K_2), K_3) \end{aligned}$$

However, we can see that, $b = F(F(0, K_3), K_2)$, so we can remove the middle 2 terms, we can now get

$$a \oplus c = F(0, K_3) \oplus F(b \oplus F(F(b, K_1), K_2), K_3)$$

Also, in this term, we can change $b \oplus F(F(b, K_1), K_2)$ to d, so we rewrite again to

$$a \oplus c = F(0, K_3) \oplus F(d, K_3)$$

Finally, if we then insert this into f, we get

$$\begin{aligned} f &= d \oplus F(F(0, K_3) \oplus F(d, K_3) \oplus F(d, K_3), K_2) \\ &= d \oplus F(F(0, K_3), K_2) \\ &= d \oplus b \end{aligned}$$

Question 2

(a) The ideal version is a random permutation.

(b) We can give a random input, and then swap the two halves and input it again, and then we can see exactly what the plaintext is. this works because the right half is unchanged in a 1 round Feistel structure.

(c) The random permutation would have to return the right half completely unchanged twice, the probability of that is $\frac{1}{2^{\frac{\ell}{2}}} \cdot \frac{1}{2^{\frac{\ell}{2}}} = \frac{1}{2^{\ell}}$

(d) The advantage as defined in slide is 2 in this case, because the computational complexity is only 2.

(e) You only need 2 executions to break it, so the security strength is 2 bits

(f) Clearly no, since it's not even PRP secure. SPRP is a stronger claim then PRP secure.