Introduction to Cryptography: Assignment 3

Group number 57

Elwin Tamminga s1013846
Lucas van der Laan s1047485

1

(a) $C_L = P_L \oplus F(K_1, P_R) \oplus F(K_3, P_R \oplus F(K_2, P_L \oplus F(K_1, P_R)))$
$C_R = P_R \oplus F(K_2, P_L \oplus F(K_1, P_R))$

(b) $P_L = C_L \oplus F(K_3, C_R) \oplus F(K_1, C_R \oplus F(K_2, C_L \oplus F(K_3, C_R)))$
$P_R = C_R \oplus F(K_2, C_L \oplus F(K_3, C_R))$

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

$b = 0^l \oplus F(K_2, 0^l \oplus F(K_3, 0^l))$
$b = F(K_2, F(K_3, 0^l))$

(d) $c = 0^l \oplus F(K_1, b) \oplus F(K_3, b \oplus F(K_2, 0^l \oplus F(K_1, b)))$
$c = F(K_1, F(K_2, F(K_3, 0^l))) \oplus F(K_3, F(K_2, F(K_3, 0^l)) \oplus F(K_2, F(K_1, F(K_2, F(K_3, 0^l)))))$

$d = b \oplus F(K_2, 0^l \oplus F(K_1, b))$
$d = F(K_2, F(K_3, 0^l)) \oplus F(K_2, F(K_1, F(K_2, F(K_3, 0^l))))$

(e) $a \oplus c =$
$F(K_3, 0^l) \oplus F(K_1, F(K_2, F(K_3, 0^l))) \oplus F(K_1, F(K_2, F(K_3, 0^l)))$
$\oplus$
$F(K_3, F(K_2, F(K_3, 0^l)) \oplus F(K_2, F(K_1, F(K_2, F(K_3, 0^l)))))$

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

$e = (a \oplus c) \oplus F(K_3, d) \oplus F(K_1, d \oplus F(K_2, (a \oplus c) \oplus F(K_3, d)))$

$e = F(K_3, 0^l) \oplus$
$F(K_3, F(K_2, F(K_3, 0^l)) \oplus$

$F(K_2, F(K_1, F(K_2, F(K_3, 0^l))))) \oplus$
$F(K_3, F(K_2, F(K_3, 0^l)) \oplus F(K_2, F(K_1, F(K_2, F(K_3, 0^l))))) \oplus$
$F(K_1, F(K_2, F(K_3, 0^l)) \oplus F(K_2, F(K_1, F(K_2, F(K_3, 0^l)))) \oplus$
$F(K_2, F(K_3, 0^l) \oplus F(K_3, F(K_2, F(K_3, 0^l)) \oplus F(K_2, F(K_1, F(K_2, F(K_3, 0^l))))) \oplus$
$F(K_3, F(K_2, F(K_3, 0^l)) \oplus F(K_2, F(K_1, F(K_2, F(K_3, 0^l)))))))$

$e = F(K_3, 0^l) \oplus F(K_1, F(K_2, F(K_3, 0^l)) \oplus F(K_2, F(K_1, F(K_2, F(K_3, 0^l))))) \oplus F(K_2, F(K_3, 0^l) \oplus$
$F(K_3, F(K_2, F(K_3, 0^l)) \oplus F(K_2, F(K_1, F(K_2, F(K_3, 0^l))))) \oplus F(K_3, F(K_2, F(K_3, 0^l)) \oplus$
$F(K_2, F(K_1, F(K_2, F(K_3, 0^l)))))))$

$e = F(K_3, 0^l) \oplus F(K_1, F(K_2, F(K_3, 0^l)) \oplus F(K_2, F(K_1, F(K_2, F(K_3, 0^l))))) \oplus F(K_2, F(K_3, 0^l)))$

$f = d \oplus F(K_2, (a \oplus c) \oplus F(K_3, d))$

$f =$
$F(K_2, F(K_3, 0^l)) \oplus F(K_2, F(K_1, F(K_2, F(K_3, 0^l)))) \oplus$
$F(K_2, F(K_3, 0^l) \oplus$
$F(K_3, F(K_2, F(K_3, 0^l)) \oplus F(K_2, F(K_1, F(K_2, F(K_3, 0^l))))) \oplus F(K_3, F(K_2, F(K_3, 0^l)) \oplus$
$F(K_2, F(K_1, F(K_2, F(K_3, 0^l))))))$

$f = F(K_2, F(K_3, 0^l)) \oplus F(K_2, F(K_1, F(K_2, F(K_3, 0^l)))) \oplus F(K_2, F(K_3, 0^l))$
$\implies f = F(K_2, F(K_3, 0^l)) \oplus F(K_2, F(K_3, 0^l)) \oplus F(K_2, F(K_1, F(K_2, F(K_3, 0^l))))$
$f = F(K_2, F(K_1, F(K_2, F(K_3, 0^l))))$

(f) $f = b \oplus d$
$f = F(K_2, F(K_3, 0^l)) \oplus F(K_2, F(K_3, 0^l)) \oplus F(K_2, F(K_1, F(K_2, F(K_3, 0^l))))$
$f = F(K_2, F(K_1, F(K_2, F(K_3, 0^l))))$

This is the same as the formula f, so indeed $f = b \oplus d$.

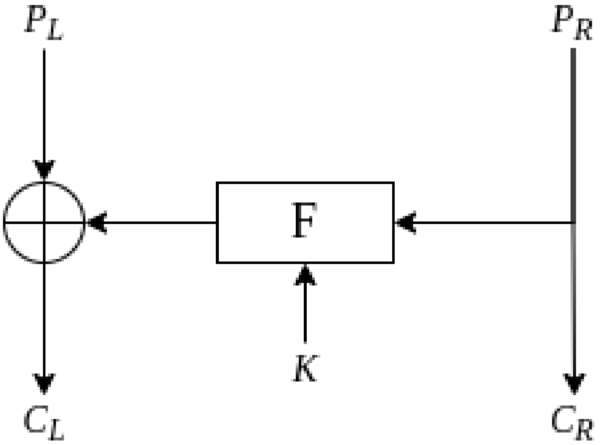
(g)

$$Adv(A_1) = |Pr[A_1 = 1|B_k] - Pr[A_1 = 1|RP]| = 1 - \frac{1}{2^l}$$

(h) It depends on the length of the key and the length of the output, so the security strength is $|K_1| + |K_2| + |K_3|$ bits.

2

(a) The ideal one round feistel structure can be seen below



(b) We encrypt $0^l||0^l$ and call the result $a||b$
We say that we are interacting with the one round Feistel structure if $b = 0^l$, and and we are interacting with the random permutation if this is not the case.

This works because P_R always directly goes to C_R.
So if the input is 0^l or 1^l, the chance of the random permutation to get that is significantly low, so you can assume that you are talking to the Feistel Structure if $C_R = P_R$.

(c) The probability is $\frac{1}{2^l}$

(d)

$$Adv(A_2) = |Pr[A_2 = 1|B_k] - Pr[A_2 = 1|RP]| = 1 - \frac{1}{2^l}$$

(e) The upper bound security strength is $|K|$ bits.

(f) No, we showed that the one round cipher is not PRP secure (which also implies that it is not SPRP secure), because the advantage of the one round cipher $Adv(A_2)$ is ≥ 0.5. The three round Feistel, using encryption and decryption queries, also has an advantage of $Adv(A_2) = Adv(A_1)$, so the three round Feistel is also not SPRP secure.