

Q1. [25pnts] For the simplified DES, consider Sbox S0 and show how DiffCrypto attack would work. Show your work for partial credit.

Table 1

x_i	y_i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0000	01	00	10	01	11	10	00	11	01	01	10	11	00	00	10	10	11
0001	11	00	10	01	11	10	00	11	01	00	11	10	01	00	10	01	00
0010	00	00	10	01	11	10	00	11	01	10	01	00	11	11	10	01	11
0011	10	00	10	01	11	10	00	11	01	11	00	01	10	00	01	01	11
0100	11	00	10	01	11	10	00	11	01	10	00	00	01	11	00	01	10
0101	01	00	10	01	11	10	00	11	01	10	00	11	10	10	01	00	11
0110	10	00	10	01	11	10	00	11	01	01	00	11	01	00	11	10	01
0111	00	00	10	01	11	10	00	11	01	10	11	11	01	01	10	11	00
1000	00	00	10	01	11	10	00	11	01	11	00	10	11	01	10	00	00
1001	11	00	11	10	01	00	01	01	00	00	10	01	11	10	00	11	01
1010	10	00	11	10	01	01	00	11	01	10	00	11	01	00	10	01	11
1011	01	00	11	10	01	11	10	10	00	11	01	10	00	01	11	00	10
1100	01	00	10	10	11	01	10	11	00	10	00	11	01	00	10	01	11
1101	11	00	10	01	00	00	11	10	01	10	00	11	01	00	10	01	11
1110	11	00	01	10	00	01	10	11	00	00	11	00	10	11	01	10	00
1111	10	00	01	01	11	11	00	01	10	10	00	11	01	00	10	01	11

Table 2

x_i	0	1	2	3
0000	16	0	0	0
0001	0	2	10	4
0010	0	10	6	0
0011	2	4	0	10
0100	2	4	8	2
0101	10	0	4	2
0110	0	2	2	12
0111	4	10	2	0
1000	2	4	8	2
1001	0	2	2	4
1010	4	2	2	8
1011	2	8	4	2
1100	8	2	2	4
1101	2	4	8	2
1110	2	8	4	2
1111	4	2	2	8

For the differential cryptoanalysis attack you first select a pair of inputs and you obtain the encrypted output of those inputs. The pair should (x, x^*) such that $X \oplus X^* = X'$ from table 1. Then create a list of inputs from Table 1 that can match the XOR of X and X^* . This leave you with a list of possible keys. Repeat the above process with a different pair of inputs. Then you compare the set of possible keys between the 2 input pairs and remove any keys that overlap. Repeat until only one key remains, this is your key.

Q2.[25pts] Consider the crypto system below and compute $H(K|C)$

$$\bullet \text{ 2) } H(K|C) = H(K) + H(P) - H(C)$$

$$I_a \quad P_r[a] = \frac{1}{3}, \quad P_r[b] = \frac{1}{6}, \quad P_r[c] = \frac{1}{2}$$

$$H(P) = \frac{1}{3} \log_2 3 + \frac{1}{6} \log_2 6 + \frac{1}{2} \log_2 2 = 1.459$$

$$H(K) = \frac{1}{2} \log_2 2 + \frac{1}{4} \log_2 4 + \frac{1}{4} \log_2 4 = 1.5$$

$$.5 + .5 + .5$$

Probability of $P_r(K=k_1)P_r(X=a) + P_r(K=k_2)P_r(X=b) + P_r(K=k_3)P_r(X=c)$

$$\frac{1}{2} \cdot \frac{1}{3} + \frac{1}{4} \cdot \frac{1}{2} = \frac{1}{6} + \frac{1}{8} = \frac{7}{24} \quad (1)$$

$$\frac{1}{2} \cdot \frac{1}{6} + \frac{1}{2} \cdot \frac{1}{2} + \frac{1}{4} \cdot \frac{1}{3} = \frac{1}{12} + \frac{1}{4} + \frac{1}{12} = \frac{5}{12} \quad (2)$$

$$\frac{1}{4} \cdot \frac{1}{3} + \frac{1}{4} \cdot \frac{1}{6} = \frac{1}{12} + \frac{1}{24} = \frac{3}{24} = \frac{1}{8} \quad (3)$$

$$\frac{1}{4} \cdot \frac{1}{6} + \frac{1}{2} \cdot \frac{1}{4} = \frac{1}{24} + \frac{1}{8} = \frac{1}{6} \quad (4)$$

$$c) = - \frac{7}{24} \log_2 \frac{7}{24} - \frac{5}{12} \log_2 \frac{5}{12} - \frac{1}{8} \log_2 \frac{1}{8} - \frac{1}{6} \log_2 \frac{1}{6}$$

$$\downarrow \quad \downarrow$$

$$.518468871 - (-.526264358) - (-.375) - (-.430)$$

$$1.851$$

$$H(K|C) = 1.5 + 1.459 - 1.851 = \boxed{1.108}$$