Crypto HW1.2

Milena Gonzalez

September 2018

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

Because we are working with only 4 bits, we know our search space is 4x4, much smaller than that of the example in the kocdiffcryptoattack.pdf. First, pick an arbitrary input XOR val from 0-15. Let's choose 2 or 0010. Now, generate plain text pairs that XOR to 2, the arbitrary input XOR. Iterate over all possible binary representations of the given search space(0-15) and XOR with 2, the arbitrary input value. We can use both the plain text values and the XORed values to get two different values from the s box in the same manor as DES. Then, XOR those two values together and create a distribution table base on what XORed values yielded each of the outputted values. For example: plain text 0 and XOR val 2 yield 1. Now, chose a specific pair from the numbers that did not yield 2, the input XOR. For example 1 and 3 because in this case, 1xor3=2. XOR one of these values, let's say 1, by all the numbers that yielded 2, the same input XOR. This will give you a set of possible key values. Repeat the process and the sets will decrease in size. The intersection will be the key value.

Q2. [25pnts] Consider the crypto system below and compute H(K—C)

- P={a,b,c} with PP(a)=1/3 PP(b)=1/6 PP(c)=1/2
- K = (k1,k2,k3) with PK(k1)=1/2 PK(k2)=1/4 PK(k3)=1/4
- C = {1,2,3,4}

e_{k_1}(a)=1	e_{k_1}(b)=2	e_{k_1}(c)=2
e_{k_2}(a)=2	e_{k_2}(b)=3	e_{k_2}(c)=1
e_{k_3}(a)=3	e_{k_3}(b)=4	e_{k_3}(c)=4

$\mathrm{H}(k_1|C_1) = \frac{P(k_1 \cap C_1)}{P(C_1)} = \frac{\frac{1}{6}}{\frac{1}{6}+\frac{1}{8}} = \frac{4}{7}$
$\mathrm{H}(k_2|C_1) = \frac{P(k_2 \cap C_1)}{P(C_1)} = \frac{\frac{1}{8}}{\frac{1}{6}+\frac{1}{8}} = \frac{3}{7}$
$\mathrm{H}(k_3|C_1) = 0$

$\mathrm{H}(k_1|C_2) = \frac{P(k_1 \cap C_2)}{P(C_2)} = \frac{\frac{1}{12}+\frac{1}{4}}{\frac{1}{4}+\frac{1}{12}+\frac{1}{12}} = \frac{\frac{4}{12}}{\frac{5}{12}} = \frac{4}{5}$
$\mathrm{H}(k_2|C_2) = \frac{P(k_2 \cap C_2)}{P(C_2)} = \frac{\frac{1}{12}}{\frac{5}{12}} = \frac{1}{5}$
$\mathrm{H}(k_3|C_2) = 0$

$\mathrm{H}(k_1|C_3) = 0$
$\mathrm{H}(k_2|C_3) = \frac{\frac{1}{24}}{\frac{1}{12}+\frac{1}{24}} = \frac{1}{3}$
$\mathrm{H}(k_3|C_3) = \frac{\frac{1}{12}}{\frac{1}{12}+\frac{1}{24}} = \frac{2}{3}$

$\mathrm{H}(k_1|C_4) = 0$
$\mathrm{H}(k_2|C_4) = 0$
$\mathrm{H}(k_3|C_4) = 1$