CS641 : Mid Semester Examination Solution

Maximum Marks: 100 **Duration: 2 hours**

Question 1 [60+40] Consider a variant of DES algorithm, called DES-WEAK. In DES-WEAK, there is no permutation P in a round and all the S-boxes are replaced. The new S-boxes are all identical and defined as follows. Let b_0, ..., b_5 represent the six input bits to an S-box and a_0, a_1, a_2, and a_3 the four output bits. Then, $a_0 = b_3 \oplus b_0b_1b_5$, $a_1 = b_0 \oplus b_1b_3b_5$, $a_2 = b_1 \oplus b_2b_3b_5$, and $a_3 = b_2 \oplus b_4 \oplus b_1b_3b_5$.

- Design an algorithm to break 16-round DES-WEAK as efficiently as possible. [60]
- Find a linear equation satisfied by 16-round DES-WEAK with as high probability as possible. The equation should only have input bits, output bits and key bits. [40]

Answer, part 1. We use differential cryptanalysis to recover the key. Consider the differential 000100 going into the S-box S2. Let one of the two inputs with the given differential be $b_0b_1b_2b_3b_4b_5$ and the corresponding output be $a_0a_1a_2a_3$. Let the output for second input $(= b_0b_1b_2b_2(b_3 \oplus 1)b_4b_5)$ be $a'_0a'_1a'_2a'_3$. Then, $a_0 \oplus a'_0 = 1$, $a_1 \oplus a'_1 = b_1b_5$, $a_2 \oplus a'_2 = b_2b_5$ and $a_3 \oplus a'_3 = b_1b_5$. Hence the output differential is 1000 on the given input differential with probability $\frac{1}{2} + \frac{1}{2} \cdot \frac{1}{4} = \frac{5}{8}$ (either b_5 is zero or b_5 is one and both b_1, b_2 are zero).

The problem with this differential output is that, in the next round, after expansion, two S-boxes will get non-zero differential. Assume that, in the first round, the differential into S1 is 000000 and the left half differential is also all zeroes. Then, in the next round, differential into S1 would be 000001 and into S2 would be 010000. Let us analyze both. First consider S1. With the same notation for first input and the two outputs (now the second input is $b_0b_1b_2b_3b_4(b_5 \oplus 1)$), we get $a_0 \oplus a'_0 = b_0b_1$, $a_1 \oplus a'_1 = b_1b_3$, $a_2 \oplus a'_2 = b_2b_3$ and $a_3 \oplus a'_3 = b_1b_3$. Hence the output diffrential is 0000 with probability $\frac{1}{2} \cdot \frac{3}{4} + \frac{1}{2} \cdot \frac{1}{4} = \frac{1}{2}$ (either b_3 is zero and one of b_0, b_1 is zero or b_3 is one and both b_1, b_2 are zero).

Consider S2. Now the second input is $b_0(b_1 \oplus 1)b_2b_3b_4b_5$, and so we get $a_0 \oplus a'_0 = b_0b_5$, $a_1 \oplus a'_1 = b_3b_5$, $a_2 \oplus a'_2 = 1$ and $a_3 \oplus a'_3 = b_3b_5$. Hence the output diffrential is 0010 with probability $\frac{1}{2} + \frac{1}{2} \cdot \frac{1}{4} = \frac{5}{8}$ (either b_5 is zero or b_5 is one and both b_0, b_3 are zero). In the next round, after applying expansion, the differential into these two S-boxes becomes 000000 000100 which is exactly the same differential that went into the first round into these two! Using this analysis, we can now derive a charecteristic with high probability as follows.

Let Z stand for zero differential on 32 bits, P stand for differential

0000 0010 0000 0000 0000 0000 0000 0000

, and $\hat{P}$ stand for differential

0000 1000 0000 0000 0000 0000 0000 0000

. The above analysis shows the following transformation sequence of differentials:

$$[P, Z] \xrightarrow{p=1} [Z, P] \xrightarrow{p=\frac{5}{8}} [P, \hat{P}] \xrightarrow{p=\frac{5}{16}} [\hat{P}, Z] \xrightarrow{p=1} [Z, \hat{P}] \xrightarrow{p=\frac{5}{16}} [\hat{P}, P] \xrightarrow{p=\frac{5}{8}} [P, Z].$$

The overall probability of the above charecteristic is $\frac{5^4}{2^{14}}$. Iterating this once again, and then taking only the first two rounds of this, we get a fourteen round charecteristic with probability $\frac{5^9}{2^{31}} \approx 9 \times 10^{-4}$. Hence using a few thousand plaintext pairs, DES-WEAK can be broken.

Answer, part 2. Notice that we have a linear equation across S-boxes that holds with probability 1: $a_1 \oplus a_3 = b_0 \oplus b_2 \oplus b_4$. We use this to derive a linear equation for one round. Let $[L_i, R_i]$ be input to $(i+1)$th round and K_{i+1} be the key used in the round. Using the notation defined in the class, and the above linear equation across all eight S-boxes, we get the linear equation:

$$R_i[1,3,5,\ldots,31] \oplus K_{i+1}[0,2,4,\ldots,46] = R_{i+1}[1,3,5,\ldots,31] \oplus L_i[1,3,5,\ldots,31],$$

which holds with probability 1. Putting together such equations for all sixteen rounds and using the fact that $L_i = R_{i-1}$, we get:

$$\begin{aligned} R_0[1,3,5,\ldots,31] \oplus L_0[1,3,5,\ldots,31] \oplus R_{16}[1,3,5,\ldots,31] \quad = \quad & \sum_{d=0}^{5} K_{3d+1}[0,2,4,\ldots,47] \oplus \\ & \sum_{d=1}^{5} K_{3d}[0,2,4,\ldots,47]. \end{aligned}$$

This equation holds with probability 1!