Laboratory work 6

Author: Dávid Kromka

Task 1

1. **Algorithm description:**

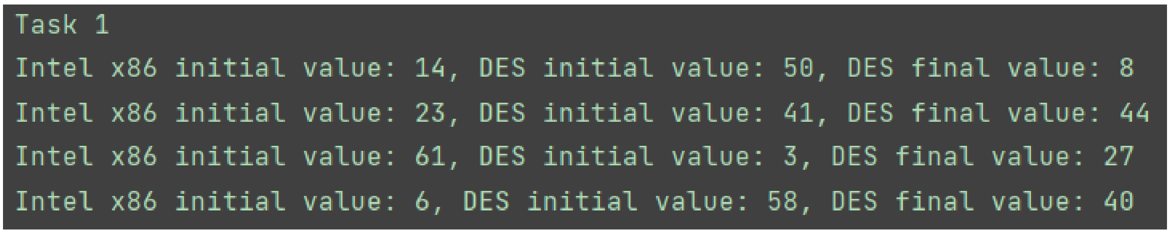
    - Inside the **tab_values()** function, there is a predefined list called **intel_values** containing Intel x86 initial values **[14, 23, 61, 6]**.
    - The algorithm iterates through each item in **intel_values**.
    - For each item, the algorithm finds its index in the **INTEL_IP** list and retrieves the corresponding DES initial and final values from the **DES_IP** and **DES_FP** lists.
    - The algorithm then prints the tabulated information in the format:
      Intel x86 initial value: {item}, DES initial value: {DES_IP[index]}, DES final value: {DES_FP[index]}

2. **Data Structures:**

    - **DES_IP**: List containing the initial permutation values for DES.
    - **DES_FP**: List containing the final permutation values for DES.
    - **INTEL_IP**: List containing the Intel x86 initial permutation values.

Output:

Element value in initial permutation table in Intel x86	Element value in initial permutation table in original DES	Element value in final permutation table in original DES
14	50	8
23	41	44
61	3	27
6	58	40



```
Task 1
Intel x86 initial value: 14, DES initial value: 50, DES final value: 8
Intel x86 initial value: 23, DES initial value: 41, DES final value: 44
Intel x86 initial value: 61, DES initial value: 3, DES final value: 27
Intel x86 initial value: 6, DES initial value: 58, DES final value: 40
```

Task 2

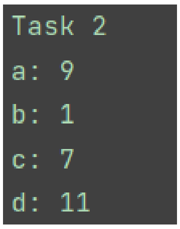
Algorithm description:

- The algorithm iterates through the list **binary_numbers** which contains binary strings **["011010", "001111", "110110", "110011"]**.
- For each binary number in **binary_numbers**:
    - The **sbox()** function is called, which extracts the outer and middle decimal values from the binary number based on specific positions.

- The extracted decimal values are used as indices to access the S-Box (**SBOX**) and retrieve the corresponding substitution result.
- The algorithm calculates the order using the **letter_counter** variable, which starts from the ASCII value of 'a' and increments with each iteration.
- The binary number, corresponding letter, and substitution result are printed in the format:
  Letter: {letter}, Binary Number: {binary_number}, S-Box Output: {result}

Output:

011010 -> 9
001111 -> 1
110110 -> 7
110011 -> 11



```
Task 2
a: 9
b: 1
c: 7
d: 11
```