COM6014

Fundamental Security Properties and Mechanisms

Assignment 1
Issued: 17 November 2022

Deadline for submission via MOLE: 1500 on 15 December 2022.

Total Marks Available 100.

The marks available for this assignment make up 50%
of the total marks available for the COM6014 module

Answer both questions.

Any queries on this assignment should be raised via the "Assessment discussion forum".

Question 1. Substitution Permutation Network Cipher and Differential Cryptanalysis (70 Marks)

A simple 3-round subs by the Heys cipher is shown in Figure 1.

The cipher operates on 8-bit blocks. Key mixing is sim it plaintext block **P** is XOR-ed bitwise with the 8-bit key K_1 before the resulti etwo first-round S-boxes. The remaining key mixing operations are handl

A substitution box (S-box) is shown in Figure 2. This S-box is used **throughout** the cipher shown in Figure 1, i.e. all 6 S-boxes are identical.

The permutation part of the first two rounds is as shown in Figure 1. The final (third) round does not implement any permutation; the outputs from the final round S-boxes are simply XOR-ed bitwise with the key $\mathbf{K_4}$ to produce ciphertext **C**.

256 plaintext-ciphertext (P-C) pairs have been generated using the 3-round cipher and four secret keys ($\mathbf{K_1}$, $\mathbf{K_2}$, $\mathbf{K_3}$, $\mathbf{K_4}$). The 256 P-C pairs are given in the file **256PC-pairs.txt** that accompanies this assessment. Plaintexts and ciphertexts are given as integers with the natural binary interpretation, e.g. the integer 5 represents the 8-bit block 00000101, 129 represents the 8-bit block 10000001, and so on.

You are required to carry out Linear Cryptanalysis on the P-C pairs provided to recover the final round key K_4.

You will need to:

a) develop one or two suitable **2-round** linear approximations for the system. You should:

i. identify the active S-boxes in your approximation(s) and their biases. Indicate how you obtained these figures. **[10 Marks]**

ii. state clearly the overall 2-round approximation(s). These will involve bits from plaintexts P, bits from intermediate ciphertexts U3, and various key bits. Formulate also related approximations that do not involve any key bits **[10 Marks]**

iii. Calculate the strength of each 2-round approximation. Give the *absolute* value of the bias of each 2-round linear approximation derived and show how they were calculated**. [8 Marks]**

iv. Identify clearly which final round key bits are targeted by each approximation. **[2 Marks]**

v. Justify your specific choices made above. **[5 Marks]**

The above allows for using one or two approximations. Different approximations may allow different final round key bits to be targeted. An approximation may allow the full 8 bits of the final round key to be targeted, or a subset of those bits (in which case you will need another approximation to discover any remaining final round bits.

Note: you should not overcomplicate your answers. You are **NOT** expected to do the step-by-step algebraic manipulations given in the lecture on Linear Cryptan is works). In answering the abo printed script it should be poss rticipating in the approximation), what individual S-box en used, and what K_4 key bits are targeted. You should suppl figure with text where necessary. You should indicate a mations both **visually AND textually**.

The above is the theoretical/analytical part of the question. You need to complete this part to inform the practical part of the question immediately below.

b) Use the results above to recover the key $\mathbf{K_4}$. Show the results of your work. You will need to implement code to:

i. read-in the P-C pairs. **[5 Marks]**

ii. carry out the (partial) decryption of ciphertexts (of PC-pairs) for a given (possibly partial) $\mathbf{K_4}$ key 'guess' (trial), i.e., to obtain the appropriate U_3 bits. **[8 Marks]**

iii. carry out the *linear approximation checking* between appropriate P bits and U_3 bits. [**8 Marks]**

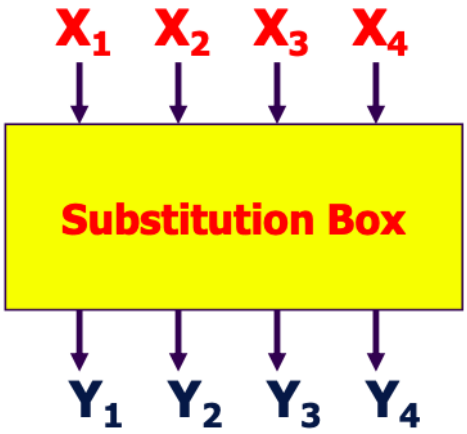
iv. identify promising candidates for K_4. You should state in your answer why identified candidate(s) are particularly promising. **[5 Marks]**

c) Outline how you would recover all remaining keys, i.e. $\mathbf{K_1}$, $\mathbf{K_2}$, and $\mathbf{K_3}$. (You are **NOT** expected to actually recover them, just outline how you would do this.) [**5 Marks**]

d) How might small changes to the algorithm shown in figure 1 improve security? **[4 Marks]**

Figure 1. Simple Very Small SPN Cipher

Input X	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Output Y	E	4	D	1	2	F	B	8	3	A	6	C	5	9	0	7



4 bit inputs and 4 bit outputs

Hex representation used

Figure 2. Specification of the Common S-Box

Question 2 Side C

This question is conce[illegible]ct cryptographic systems. Write a short report (**800 words max**) on the topic of cryptographic side channels. You should:

a) Explain what is meant by the term 'side channe[illegible]tosystems. **[5 Marks]**

b) Give brief descriptions of particular side channels. **[10 Marks]**

c) Describe countermeasures to those side channels and assess those countermeasures in terms of how effective they are and how practical it is to implement them. **[10 Marks]**

d) Research available literature on side channels and use it to inform your answer. **[5 Marks]**