

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 substitution permutation network (SPN) cipher inspired by the Heys cipher is shown in Figure 1.

The cipher operates on 8-bit blocks. Key mixing is simple bitwise XOR. The 8-bit plaintext block  $P$  is XOR-ed bitwise with the 8-bit key  $K_1$ , before the resulting 8-bit block enters the two first-round S-boxes. The remaining key mixing operations are handled similarly.

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  $K_4$  to produce ciphertext  $C$ .

256 plaintext-ciphertext (P-C) pairs have been generated using the 3-round cipher and four secret keys ( $K_1, K_2, K_3, K_4$ ). 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:
- identify the active S-boxes in your approximation(s) and their biases. Indicate how you obtained these figures. **[10 Marks]**
  - state clearly the overall 2-round approximation(s). These will involve bits from plaintexts P, bits from intermediate ciphertexts U<sub>3</sub>, and various key bits. Formulate also related approximations that do not involve any key bits **[10 Marks]**
  - 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]**
  - Identify clearly which final round key bits are targeted by each approximation. **[2 Marks]**
  - 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.

## Assignment Project Exam Help

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 Cryptanalysis (which serve to show *why* linear cryptanalysis works). In answering the above you should include a copy of figure 1 in your submitted script. It should be possible to tell at a glance which S-boxes are active (participating in the approximation), what individual S-box approximations have been used, and what K<sub>4</sub> key bits are targeted. You should supplement your annotated figure with text where necessary. You should indicate any active S-box approximations 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 K<sub>4</sub>. Show the results of your work. You will need to implement code to:
- read-in the P-C pairs. **[5 Marks]**
  - carry out the (partial) decryption of ciphertexts (of PC-pairs) for a given (possibly partial) K<sub>4</sub> key 'guess' (trial), i.e., to obtain the appropriate U<sub>3</sub> bits. **[8 Marks]**
  - carry out the *linear approximation checking* between appropriate P bits and U<sub>3</sub> bits. **[8 Marks]**
  - identify promising candidates for K<sub>4</sub>. 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. K<sub>1</sub>, K<sub>2</sub>, and K<sub>3</sub>. (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]

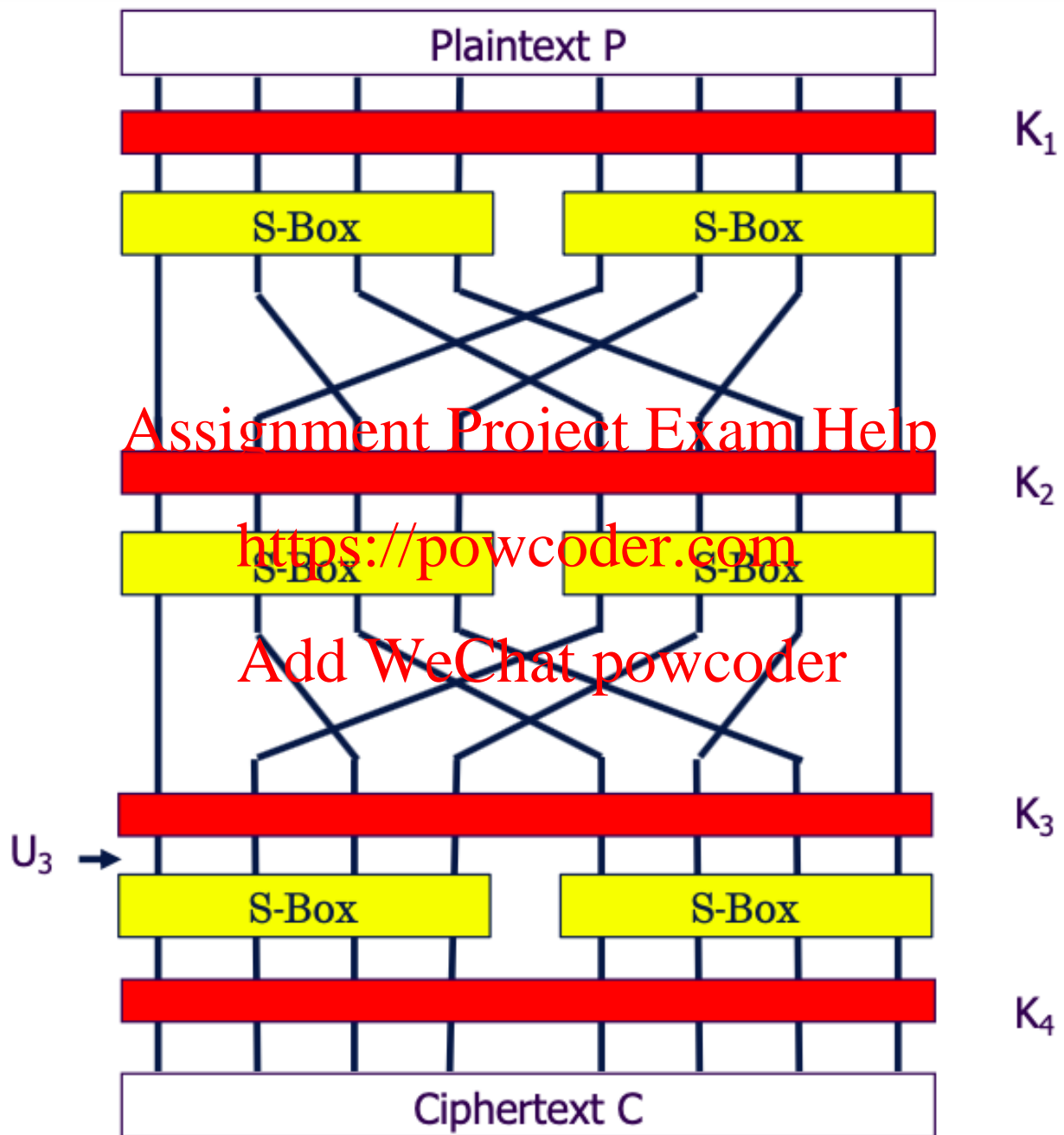


Figure 1. Simple Very Small SPN Cipher

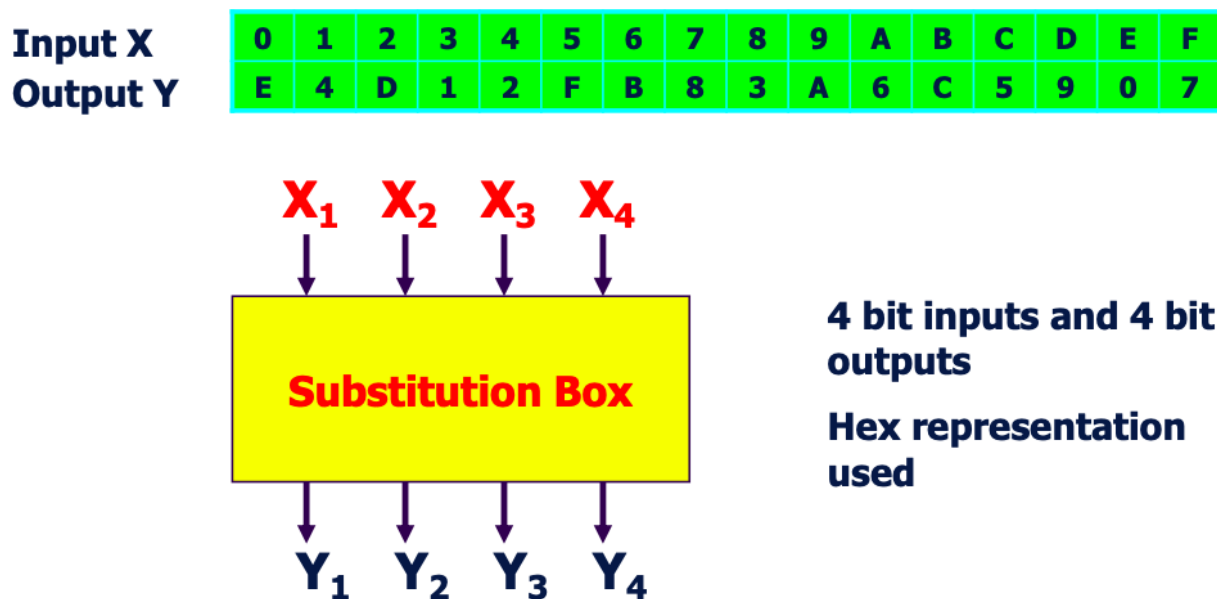


Figure 2. Specification of the Common S-Box

## Assignment Project Exam Help

### Question 2 Side Channels (30 Marks)

This question is concerned with the use of so-called "side channels" to attack cryptographic systems. Write a short report (**800 words max**) on the topic of cryptographic side channels. You should:

- Explain what is meant by the term "side channel" in the context of cryptosystems. **[5 Marks]**
- Give brief descriptions of particular side channels. **[10 Marks]**
- 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]**
- Research available literature on side channels and use it to inform your answer. **[5 Marks]**