

Fundamental Security Properties and Mechanisms

Issued: 5 September 2022

Total Marks Available 100.

Answer both questions.

Question 1. Substitution Permutation Network Cipher and Differential Cryptanalysis (60 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 **K₁** 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 **K₄** to produce ciphertext **C**.

256 plaintext-ciphertext (P-C) pairs have been generated using the 3-round cipher and four secret keys (**K₁**, **K₂**, **K₃**, **K₄**). The 256 P-C pairs are given in the file **TwoFiveSixPCs.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 Differential Cryptanalysis on the P-C pairs provided.

You should:

- a) Use **Differential Cryptanalysis** to recover the final round key **K₄**. You should:
 - i. **develop** one or more suitable **2-round** differential approximations involving bits of the plaintexts **P** and bits of intermediate ciphertexts **U₃** (as shown in **Figure 1**). [10 Marks]

- ii. **indicate** any active S-boxes in your approximations and their biases. Indicate any tables (or other sources) you have used to calculate the biases [5 Marks]
- iii. **give** the absolute value of the bias of any 2-round approximation derived above and show how all such biases were calculated. [5 Marks]
- iv. **Explain** your specific choice of approximation(s). [5 Marks]

The above allows for using two approximations: one that targets the first four bits of K_4 and one that targets the second four bits of K_4 . It also allows for the use of a single approximation that targets all 8 bits of the key K_4 . You should justify your choice.

The above is the theoretical 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_4 . Show the results of your work. You will need to **implement code to**:

- i. **read-in** the P-C pairs. [5 Marks]
- ii. **identify and use** suitable (P, C) , (P', C') , where $P \oplus P' = \Delta P$, i.e. the plaintext difference part of a differential approximation. [5 Marks]
- iii. **carry out** the (partial) decryption of pairs of relevant ciphertexts for a given (possibly partial) key guess, i.e., to obtain the appropriate U_3 bits. [10 Marks]
- iv. **carry out** the **differential approximation checking** between appropriate ΔP bits and ΔU_3 bits. [5 Marks]
- v. **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. K_1 , K_2 , and K_3 . (You are **not** expected to actually recover them, just outline how you would do this.) [5 Marks]

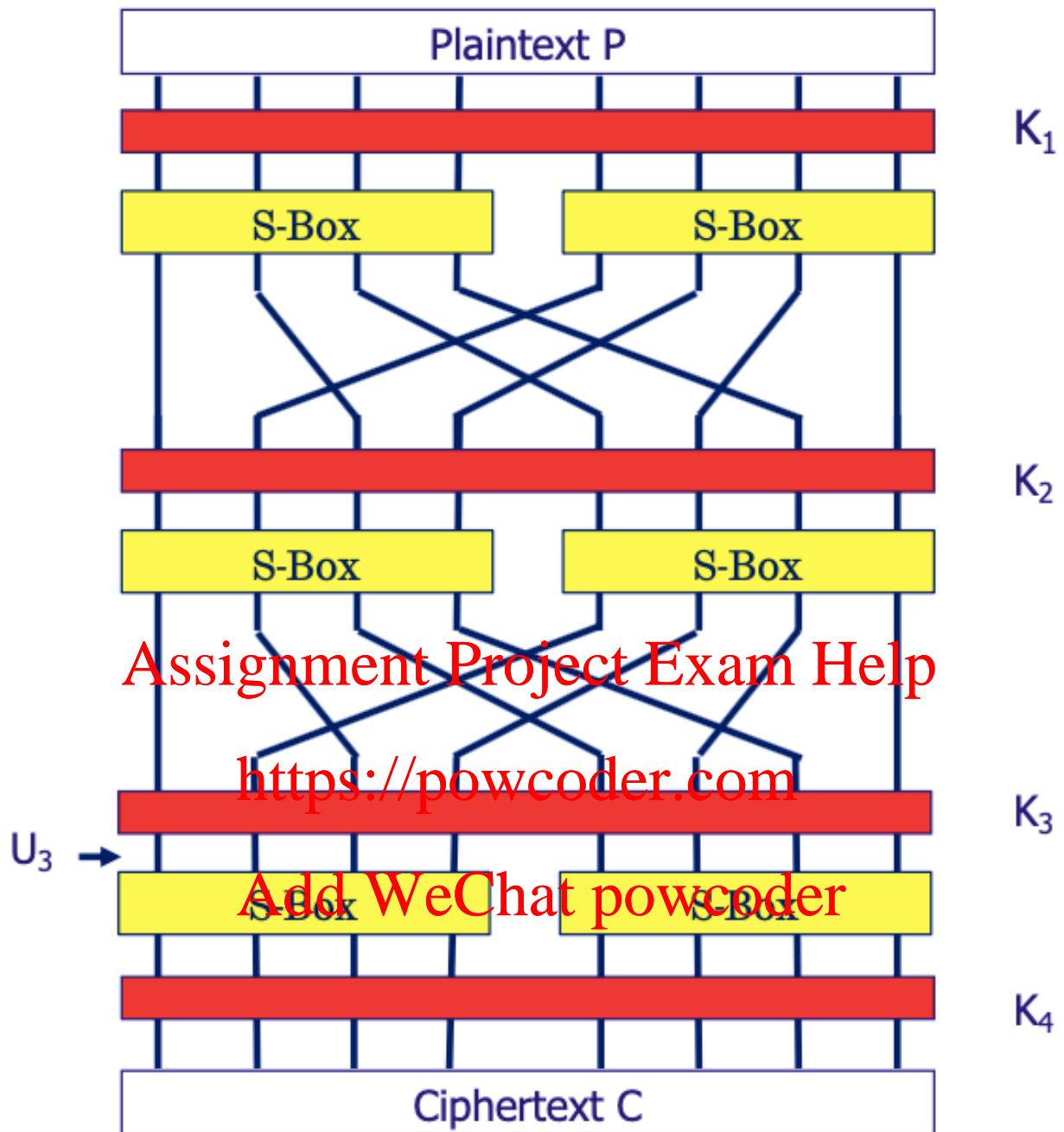


Figure 1. Simple Very Small SPN Cipher

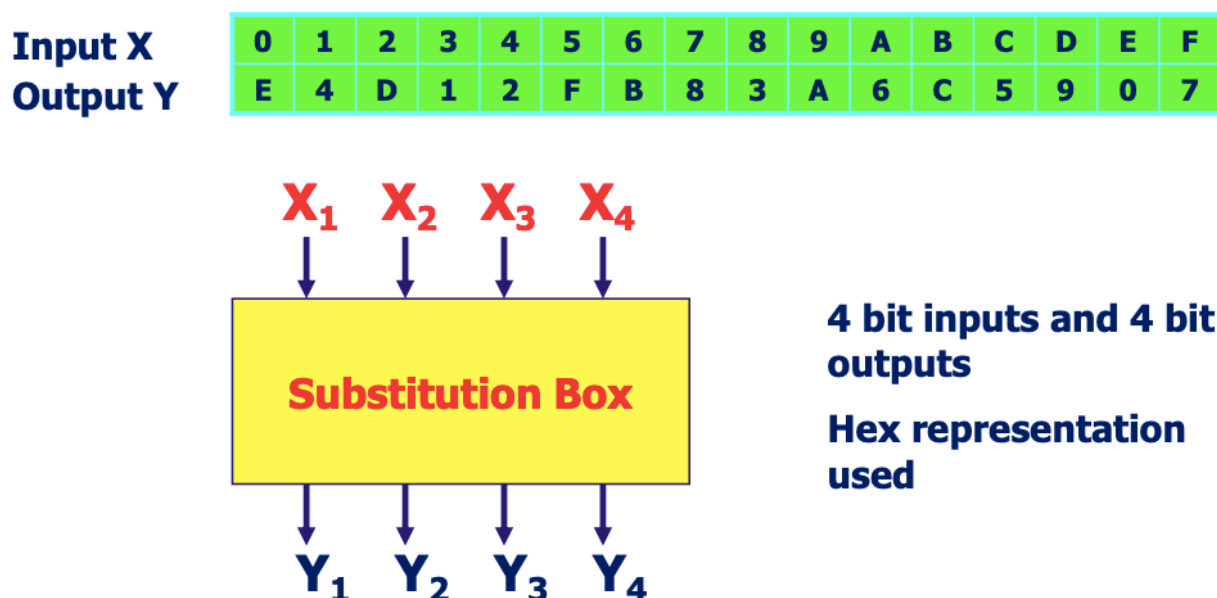


Figure 2. Specification of the Common S-Box

Assignment Project Exam Help

Q2 Podcast on Authentication (40 Marks)

You are required to produce a 'podcast' for local radio on the topic of "user authentication". The intended listeners are the general public. Accordingly, your podcast **should avoid technical jargon**. It should:

- indicate what user authentication is and why it is needed;
- identify major user authentication approaches and give illustrative examples;
- highlight some practical downsides/challenges with user authentication and how they can be addressed;
- highlight some controversial issues (or potentially controversial issues); and
- give an indication of how you see the future of user authentication in cybersecurity evolving.

Marks are awarded for:

- **Topic content.** Selection of content. Coverage of the above requirements. Is there a coherent and balanced narrative? [24 Marks]
- **Appropriate expression.** Will the **public** understand it? It is expressed in an accurate but accessible way? [8 Marks]
- **Oral delivery.** Is there a natural and engaging feel to your presentation? [8 Marks]

You should prepare a **script file** for your podcast (i.e., a file that has the textual version of your podcast content) and an audio file. [The script will allow the markers to determine what is being said if the audio is unclear.] The duration of the podcast **must** be between **2 minutes 55 seconds** and **3 minutes**. It **must** be submitted in a common audio format (mp3 preferred).

A **folder containing all necessary submission elements** should be **compressed** (using zip) and **submitted** via the MOLE site. A COM6014 blog will be maintained specifically for this assignment. Queries on this assignment should be made via that blog.