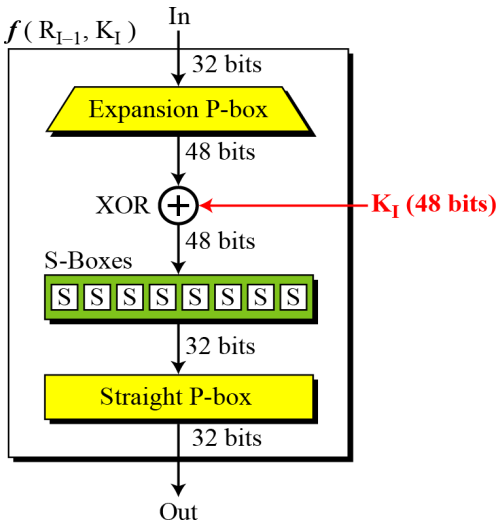
1. Define the terms "vulnerability," "threat," and "attack" in the field of information security.
   Solution:-
   Vulnerability: Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

   Threat: Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

   Attack: Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.

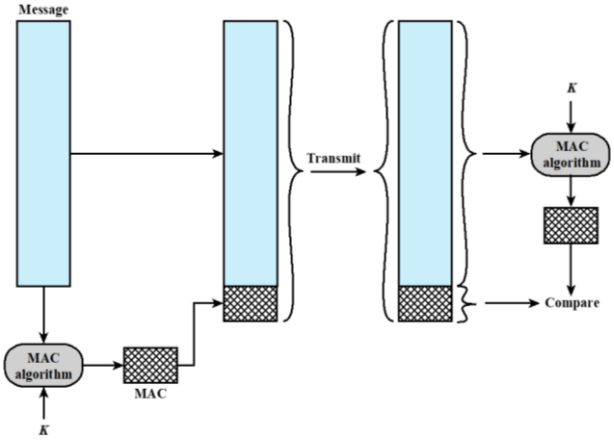
2. Explain the concept of "Least Privilege" as a fundamental security design principle. Describe how implementing the principle of Least Privilege enhances security, and provide an example scenario in which it can be applied effectively.
   Solution:-
   Grant users and processes only the minimum permissions necessary to perform their tasks. Least Privilege offers numerous security benefits, such as preventing unauthorized actions, strengthening data protection, minimizing the spread of malware. Scenario like Role Based Access Control (RBAC) Model

3. Draw a labeled diagram of the inner working of Feistel function
   Solution:-



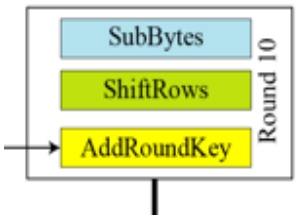
4. Alice intends to transmit a message to Bob while desiring Bob's ability to confirm that the message remained unchanged during transmission over a channel. Describe the sequence of actions that Alice and Bob need to undertake in order to safeguard the message's integrity through the creation and validation of a Message Authentication Code (MAC). (figure or explanation both answers are acceptable)

Solution:-



5. Draw a block diagram illustrating the structure of the final round in the AES encryption.

Solution:-



6. Suppose an organization implementing a secure document signing system for official documents, with the goals of authentication, maintaining document integrity, and ensuring signatory non-repudiation. Explain the processes involved in both creating and verifying these documents. (figure or explanation both answers are acceptable)

Solution:-

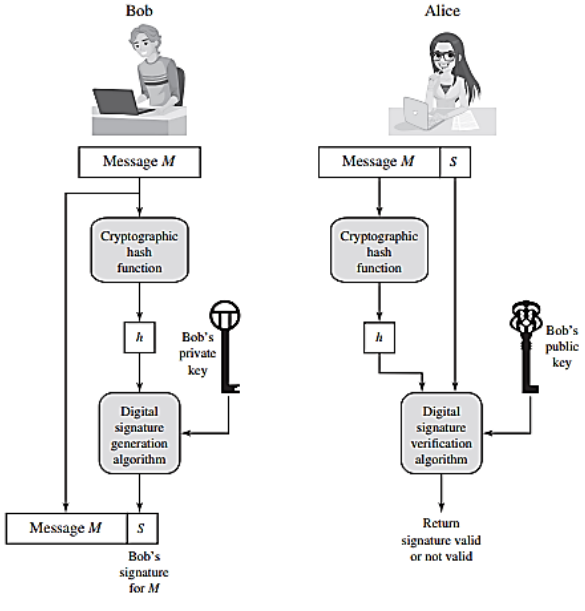


Figure 2.7 **Simplified Depiction of Essential Elements of Digital Signature Process**

7. What is implied by the statement that a function H possesses "preimage resistance"?

Solution:- For any given code h, it is computationally infeasible to find x such that H(x) h. A hash function with this property is referred to as one-way or preimage resistant