**[SEHAR ELAHI]**

[Paper Work]

[Mam Farah Naz]

**20496 (BSCS)**

**Paper Work**

**Development of Cybersecurity and** algorithm

# Topic: S-box (Sub byte)

**Definition:**

“ In [cryptography](https://en.wikipedia.org/wiki/Cryptography), an S-box (substitution-box) is a basic component of [symmetric key algorithms](https://en.wikipedia.org/wiki/Symmetric_key_algorithm)

  which performs substitution (the action of replacing something with another thing). Mathematically,

an S-box is a vectoral [Boolean function](https://en.wikipedia.org/wiki/Boolean_function)”.

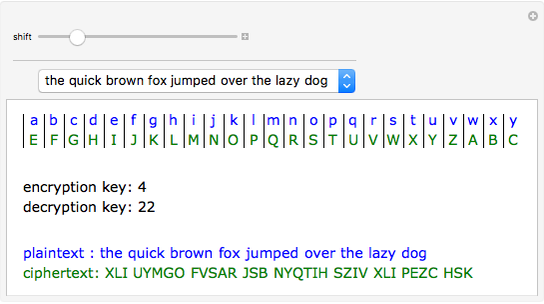
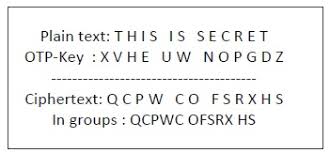
* **What is cryptography and how it works?**

A cryptographic algorithm, or cipher (unreadable output), is a mathematical function used in the encryption and decryption process. Cryptography is the science of protecting information by transforming it into a secure format.

“A cryptographic algorithm works **in combination with a key — a word, number, or**

**phrase — to encrypt the plaintext**. The same plaintext encrypts to different ciphertext with

different keys”.



In general, an S-box takes some number of input [bits](https://en.wikipedia.org/wiki/Bit), *m*, and transforms them into some number of output bits, *n*, where *n* is not necessarily equal to *m*. An (*m* × *n)*  S-box can be implemented as a [lookup table](https://en.wikipedia.org/wiki/Lookup_table).

* **Why we need S-Box?**

The **substitution bytes** (S-Box) in AES algorithm plays an important role as it provides confusion in the cipher text [10, 11]. The basic function of S-Box is to transforms the 8 bits input data into 8 bits secret data using a precomputed look-up-table (LUT).

* **What is S-Box? Why it is important?**

In block ciphers, S-box and P-box are two important components of a secure block cipher identified by Claude Shannon. The basic purpose of an S-box is **to produce confusion between the ciphertext and the secret key** and P-box is responsible for diffusion. S-box is the heart of every block cipher cryptosystem.

* A block “Cipher is a method of encrypting data in blocks to produce ciphertext using a cryptographic key and algorithm”. Most modern block ciphers are designed to encrypt data in fixed-size blocks of either 64 or 128 bits.
* **How is S-Box created in AES?**

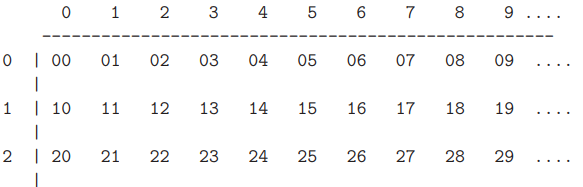
STEP 1: (called Sub Bytes for byte-by-byte substitution during the forward process)

(The corresponding substitution step used during decryption is called Inv Sub Bytes).

* This step consists of using a 16 × 16 lookup table to find a replacement byte for a given byte in the input state array.
* ˆThe entries in the lookup table are created by using the notions of multiplicative inverses in GF (28) and bit scrambling to destroy the bit-level correlations inside each byte.
* **Purpose of Substitution of bytes:**

The goal of the substitution step is to reduce the correlation between the input bits and the output bits at the byte level. The bit scrambling part of the substitution step ensures that the substitution cannot be described in the form of evaluating a simple mathematical function.

* I’ll now present the more traditional explanation of the byte substitution step. As mentioned earlier, it involves using a 16 × 16 table. To find the substitute byte for a given input byte, we divide the input byte into two 4-bit patterns, each yielding an integer value between 0 and 15. (We can represent these by their hex values 0 through F.) One of the hex values is used as a row index and the other as a column index for reaching into the 16 × 16 lookup table.
* Traditional Explanation of Byte Substitution: Constructing the 16 × 16 Lookup Table
* We first fill each cell of the 16 × 16 table with the byte obtained by joining together its row index and the column index. [The row index of this table runs from hex 0 through hex F. Likewise, the column index runs from hex 0 through hex F.] ˆ For example, for the cell located at row index 2 and column indexed 7, we place hex 0x27 in the cell. So at this point the table will look like



We next replace the value in each cell by its multiplicative inverse in GF (28) based on the irreducible polynomial.

## **Example 1**

One good example of a fixed table is the S-box from DES (S5), mapping 6-bit input into a 4-bit output:

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **S5** | | **Middle 4 bits of input** | | | | | | | |
| **Outer bits** |  | **0000** | **0001** | **0010** | **0101** | **0111** | **1101** | **1101** | **1111** |
| 00 | 0010 | 1100 | 0100 | 0001 | 0111 | 0000 | 1110 | 1001 |
| 01 | 1110 | 1011 | 0010 | 1100 | 0100 | 1001 | 1000 | 0110 |
| 10 | 0100 | 0010 | 0001 | 1011 | 1101 | 0011 | 0000 | 1110 |
| 11 | 1011 | 1000 | 1100 | 0111 | 1110 | 0100 | 0101 | 0011 |

Given a 6-bit input, the 4-bit output is found by selecting the row using the outer two bits (the first and last bits), and the column using the inner four bits. For example, an input "**0**1101**1**" has outer bits "**01**" and inner bits "1101"; the corresponding output would be "1001".

The eight S-boxes of DES were the subject of intense study for many years out of a concern that a [*backdoor*](https://en.wikipedia.org/wiki/Backdoor_(computing)) (a [vulnerability](https://en.wikipedia.org/wiki/Cryptanalysis) known only to its designers) might have been planted in the cipher. The S-box design criteria were eventually published (in [Coppersmith 1994](https://en.wikipedia.org/wiki/S-box#CITEREFCoppersmith1994)) after the public rediscovery of [differential cryptanalysis](https://en.wikipedia.org/wiki/Differential_cryptanalysis), showing that they had been carefully tuned to increase resistance against this specific attack. Bilham and Shamir found that even small modifications to an S-box could significantly weaken DES.

## **Analysis and properties**

There has been a great deal of research into the design of good S-boxes, and much more is understood about their use in block ciphers than when DES was released.

Any S-box where any linear combination of output bits is produced by a Boolean, the input bits is termed a **perfect S-box**.

AES data encryption is a more mathematically efficient and elegant cryptographic algorithm, but its main strength rests in the option for various key lengths. AES allows you to choose a 128-bit, 192-bit or 256-bit key, making **it exponentially stronger than** the 56-bit key of DES.

**Key Length:**56 bits

**Cipher Type:**Symmetric block cipher

**Block Size:**64 bits

## **Example 2**

