

**Spring Semester 2021**

**CSE463M-563M: Digital Integrated Circuit Design and Architecture**

**Simplified Data Encryption Standard Algorithm**

**Data Encryption has been very important part of data security for a long time. From financial services, to military products and everything in between all require some kind of data encryption and everybody wants a bullet proof type of data encryption.**

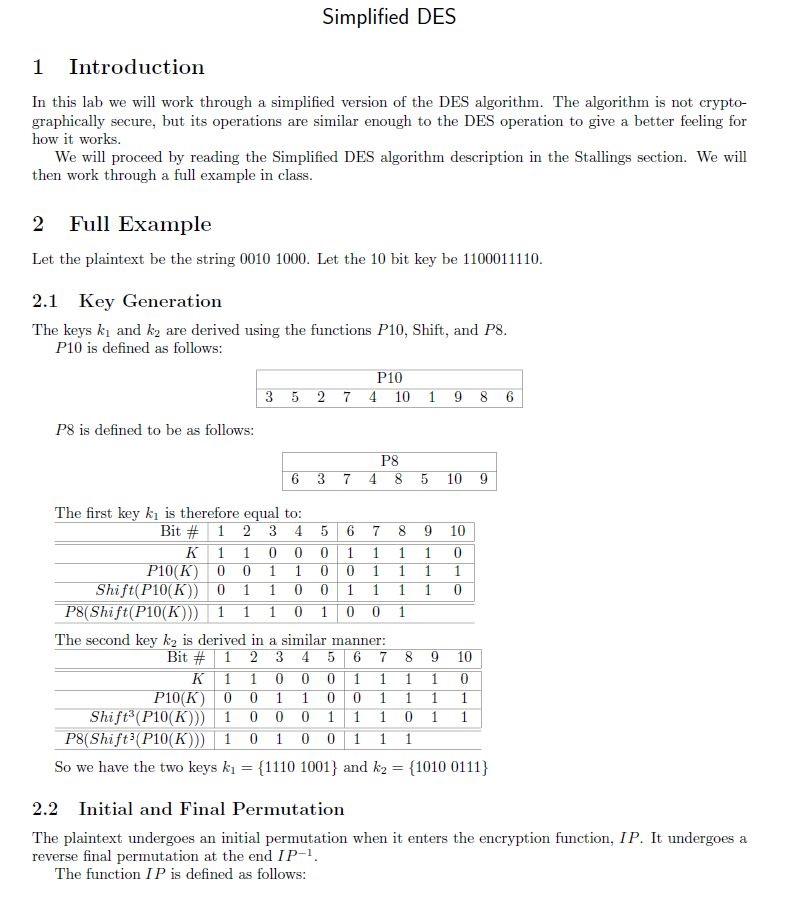
**One of the important Data Encryption algorithms was Data Encryption Standard (DES) which was developed at IBM in the early 1970. National Security Agency (NSA) selected slightly modified version of DES algorithm as an official Federal Information Processing Standard (FIPS) for the USA in 1977.**

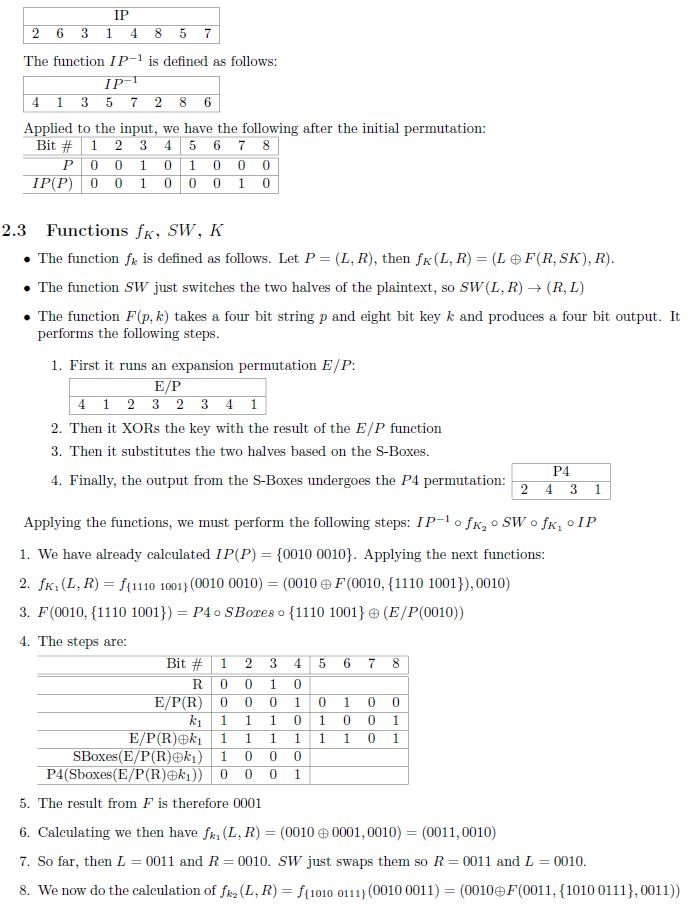
**DES algorithm had widespread academic scrutiny thru its usage and in January of 1999, distributed.net and Electronic Frontier Foundation publicly proved that they can break a DES key in 22 hours and 15 minutes. Therefore DES was replaced by the Advanced Encryption Standard (AES).**

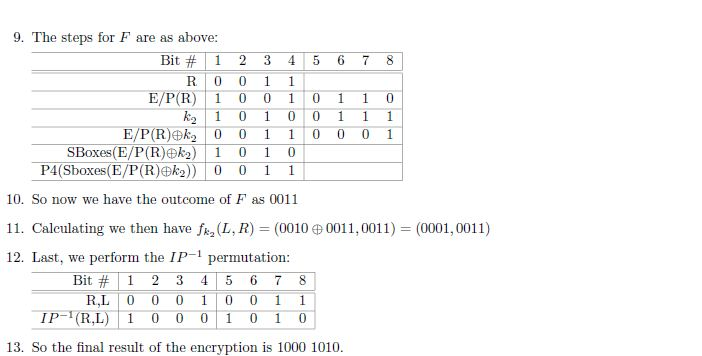
**To learn some basic design structures of encryption algorithms we will study Simplified DES algorithm which is a good starting points for undergraduate engineering students to learn some basics of encryption algorithms design.**

**First we will learn how the Simplified DES algorithm works using binary mathematics. Then we will write a simple piece of code that will show how the Simplified DES algorithm works. Finally we will design an integrated chip that will also show how the Simplified DES algorithm works in hardware.**

**Simplified DES algorithm example is shown here. This is example was borrowed from a college Security algorithms class and it can be googled easily.**

****

****

****

**SBoxes used in this example are:**

**SBox\_1 for the left 4-bits b1, b2, b3, b4 (circled twice in red)**

b2 b3 b2 b3 b2 b3 b2 b3

b1

b4

b1

b4

b1

b4

b1

b4

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 1 |
| 0 | 0 | | 0 | | 1 | | 1 | |
| 0 | 1 | | 0 | | 1 | | 0 | |
| 0 | 1 | | 1 | | 0 | | 0 | |
| 1 | 1 | | 0 | | 1 | | 0 | |
| 1 | 0 | | 1 | | 0 | | 1 | |
| 0 | 0 | | 0 | | 1 | | 1 | |
| 1 | 1 | | 0 | | 1 | | 1 | |
| 1 | 1 | | 1 | | 1 | | 0 | |

**SBox\_2 for the right 4-bits b1, b2, b3, b4 (circled twice in green)**

b2 b3 b2 b3 b2 b3 b2 b3

b1

b4

b1

b4

b1

b4

b1

b4

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 1 |
| 0 | 0 | | 0 | | 1 | | 1 | |
| 0 | 0 | | 1 | | 0 | | 1 | |
| 0 | 1 | | 0 | | 0 | | 1 | |
| 1 | 0 | | 0 | | 1 | | 1 | |
| 1 | 1 | | 0 | | 0 | | 0 | |
| 0 | 1 | | 0 | | 1 | | 0 | |
| 1 | 1 | | 0 | | 0 | | 1 | |
| 1 | 0 | | 1 | | 0 | | 1 | |