# **THIẾT KẾ LÕI IP DES (DATA ENCRYPTION STANDARD)**

## **Đặt vấn đề:**

* Trong bối cảnh an toàn thông tin ngày càng trở thành mối quan tâm hàng đầu, các thuật toán mã hóa đóng vai trò quan trọng trong việc bảo vệ dữ liệu khỏi các cuộc tấn công. Một trong những thuật toán mã hóa được sử dụng rộng rãi là Data Encryption Standard (DES), một thuật toán mã hóa khối có lịch sử lâu đời và vẫn còn ứng dụng trong nhiều hệ thống phần cứng nhúng. Mặc dù DES đã dần được thay thế bởi Advanced Encryption Standard (AES) trong các hệ thống yêu cầu độ bảo mật cao, nhưng nó vẫn giữ được giá trị trong các ứng dụng đòi hỏi tốc độ xử lý nhanh và chi phí phần cứng thấp. Việc thiết kế một lõi IP DES giúp tối ưu hóa hiệu suất xử lý mã hóa trên phần cứng như FPGA hoặc ASIC, mang lại nhiều lợi ích so với các giải pháp phần mềm chạy trên vi xử lý truyền thống. Một lõi IP DES có thể được tối ưu để đạt hiệu suất cao, tiết kiệm năng lượng và dễ dàng tích hợp vào các hệ thống nhúng, đặc biệt là trong các ứng dụng yêu cầu mã hóa nhanh chóng như truyền thông bảo mật, hệ thống nhúng công nghiệp và thiết bị IoT. Vì lý do trên, đề tài "Thiết kế lõi IP DES" nhằm mục tiêu nghiên cứu và phát triển một lõi phần cứng hiệu quả cho thuật toán DES, đáp ứng các yêu cầu về hiệu suất, tài nguyên và tính linh hoạt khi tích hợp vào các hệ thống thực tế.

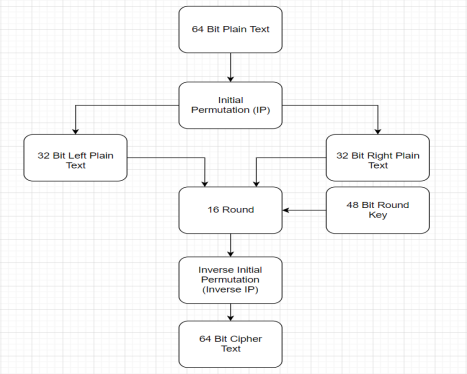
## **Giới thiệu về đề tài:**

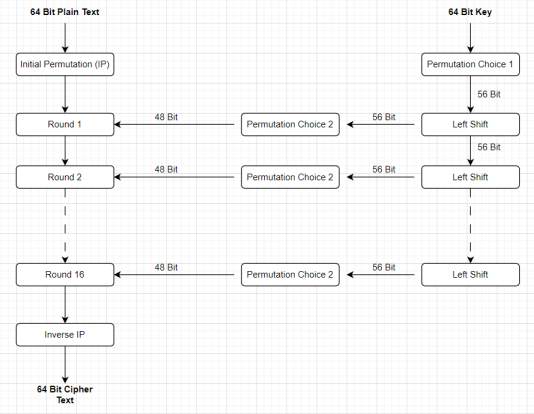
### **Lõi IP:**

* **Intellectual Property (IP)** trong VLSI là một khối logic hoặc chức năng có thể tái sử dụng, hoặc một cell, hoặc một thiết kế bố trí, thường được phát triển để sử dụng như các khối xây dựng trong các thiết kế chip khác nhau.
* Trong kỷ nguyên thiết kế vi mạch ngày nay, ngày càng nhiều chức năng hệ thống được tích hợp vào một chip duy nhất (thiết kế Hệ thống trên chip – SoC). Trong các thiết kế SoC này, các lõi IP/khối được thiết kế sẵn ngày càng trở nên quan trọng. Điều này là do hầu hết các thiết kế SoC đều có một vi xử lý tiêu chuẩn và nhiều chức năng hệ thống được tiêu chuẩn hóa, do đó, nếu được thiết kế một lần, chúng có thể được tái sử dụng trong nhiều thiết kế khác nhau.

### **Thuật toán DES:**

* Tiêu chuẩn Mã hóa Dữ liệu (DES) là một thuật toán mã hóa khối với độ dài khóa 64 bit, đóng vai trò quan trọng trong bảo mật dữ liệu. DES là một mã hóa khối và mã hóa dữ liệu theo từng khối có kích thước 64 bit, nghĩa là 64 bit văn bản gốc được đưa vào DES, sau đó tạo ra 64 bit văn bản mã hóa:
* Input: 64 bits
* Output: 64 bits
* Key: 64 bits
* Round Key: 48 bits
* No. of Round: 16 round
* DES dựa trên hai thuộc tính cơ bản của mật mã: thay thế (còn gọi là làm rối - confusion) và hoán vị (còn gọi là khuếch tán - diffusion). DES bao gồm 16 bước, mỗi bước được gọi là một vòng (round). Mỗi vòng thực hiện các bước thay thế và hoán vị. Dưới đây là các bước chính của DES:
* Ở bước đầu tiên, khối văn bản gốc 64-bit được đưa vào một hàm hoán vị ban đầu (Initial Permutation - IP).
* Sau đó, hoán vị ban đầu (IP) tạo ra hai nửa của khối đã hoán vị, gọi là Văn bản gốc bên trái (Left Plain Text - LPT) và Văn bản gốc bên phải (Right Plain Text - RPT).
* Tiếp theo, mỗi LPT và RPT trải qua 16 vòng của quá trình mã hóa.
* Cuối cùng, LPT và RPT được ghép lại và một Hoán vị cuối cùng (Final Permutation - FP) được thực hiện trên khối đã kết hợp.
* Kết quả của quá trình này tạo ra văn bản mã hóa 64-bit.





### **Kết luận:**

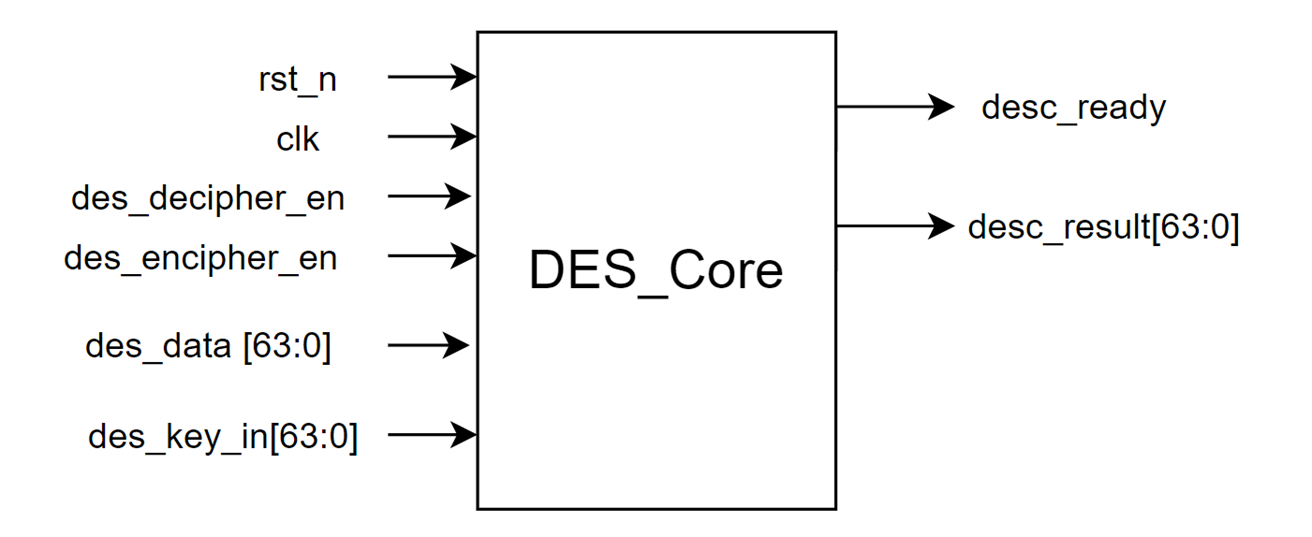
* Lõi IP (Intellectual Property) trong thiết kế vi mạch là một khối phần cứng có thể tái sử dụng, được thiết kế để thực hiện một chức năng cụ thể và có thể tích hợp vào các hệ thống trên chip (SoC) hoặc FPGA. Trong đề tài này, chúng tôi tập trung vào thiết kế lõi IP cho thuật toán mã hóa DES, một thuật toán mã hóa khối với chiều dài khóa 64-bit và kích thước khối dữ liệu 64-bit. Lõi IP DES được thiết kế nhằm đảm bảo khả năng hoạt động hiệu quả trên nền tảng phần cứng. Thiết kế này có thể áp dụng trong nhiều lĩnh vực như bảo mật truyền thông, hệ thống nhúng, thiết bị IoT và các ứng dụng yêu cầu xử lý mã hóa tốc độ cao. Đề tài sẽ tập trung vào việc phân tích, thiết kế và kiểm thử lõi IP DES bằng ngôn ngữ mô tả phần cứng Verilog.

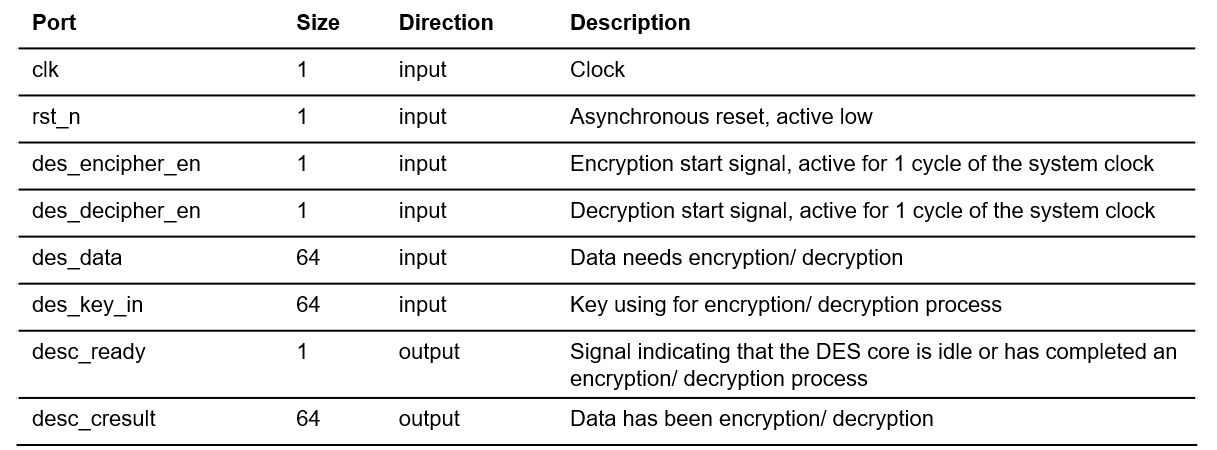
## **Thiết kế**

* Dưới đây là phần thiết kế của bộ mã hóa và giải mã

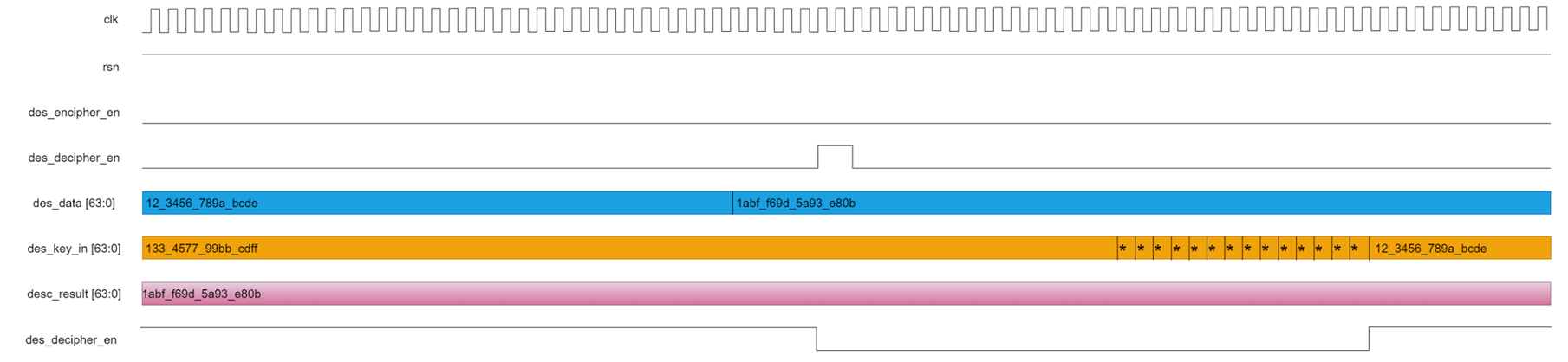
### **Signal Diagram:**

* Sơ đồ khối:



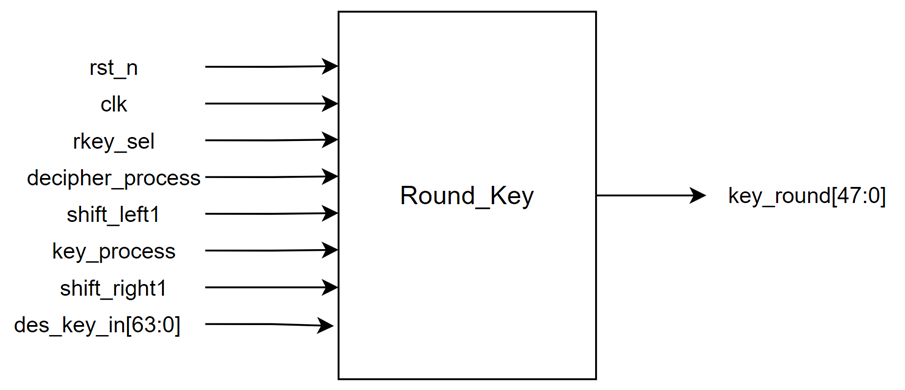


* Dạng sóng:

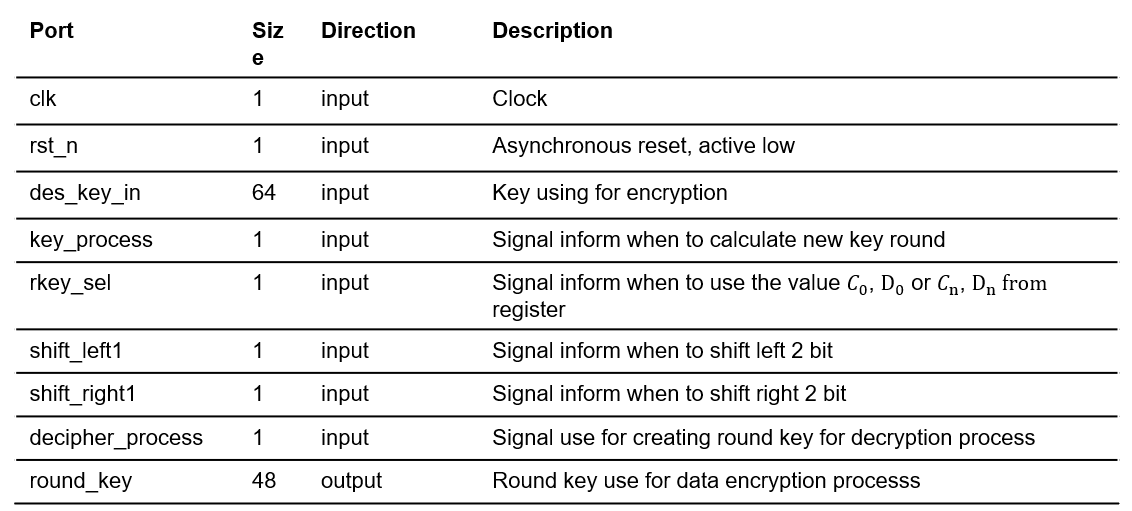


### **DES Round Key Block (Round Key Generation Circuit)**

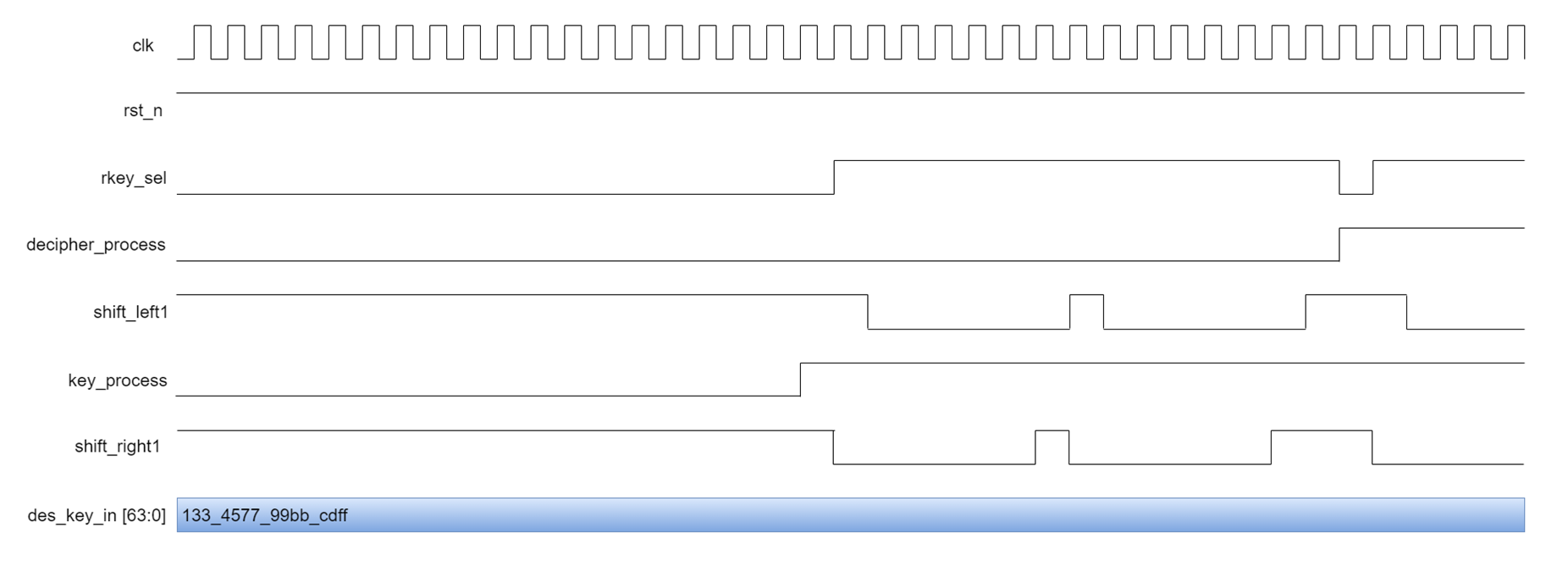
* Sơ đồ khối:



* Chức năng: Khối này chịu trách nhiệm tạo ra 16 khóa vòng từ khóa chính

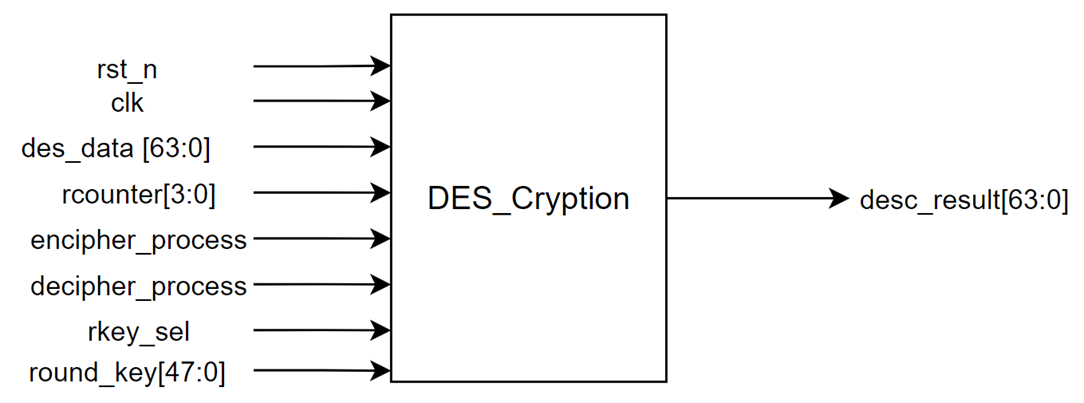


* Dạng sóng:

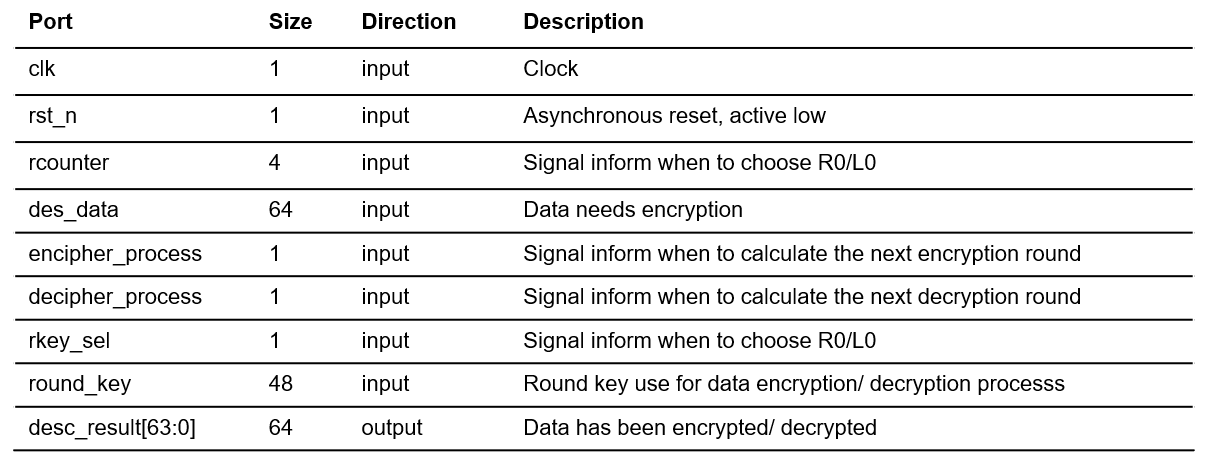


### **DES Data Encryption:**

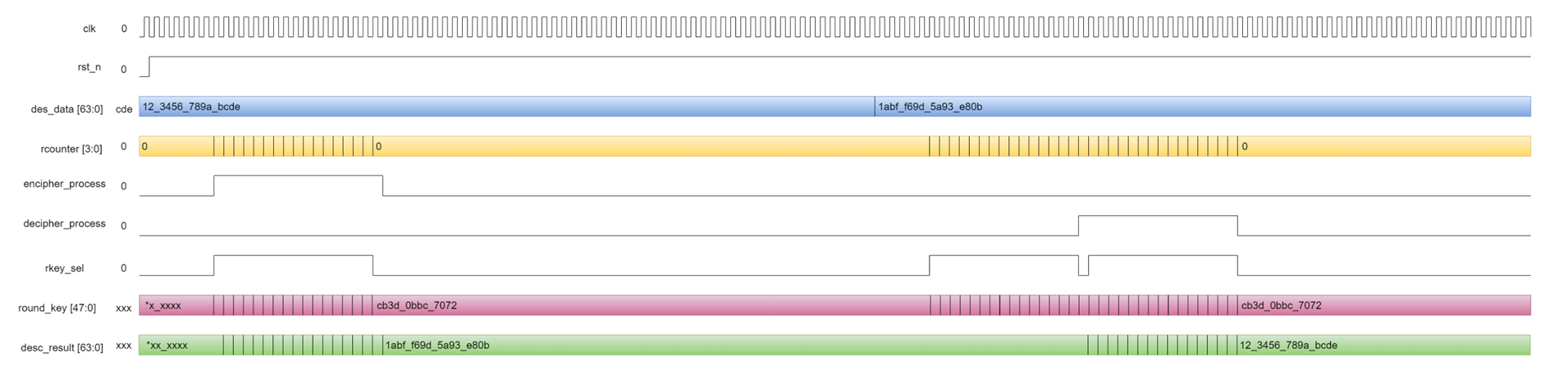
* Sơ đồ khối:



* Chúc năng: Thực hiện quá trình mã hóa/giải mã

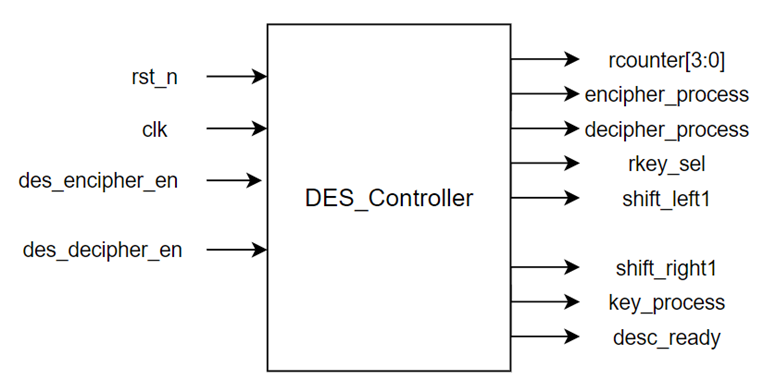


* Dạng sóng:

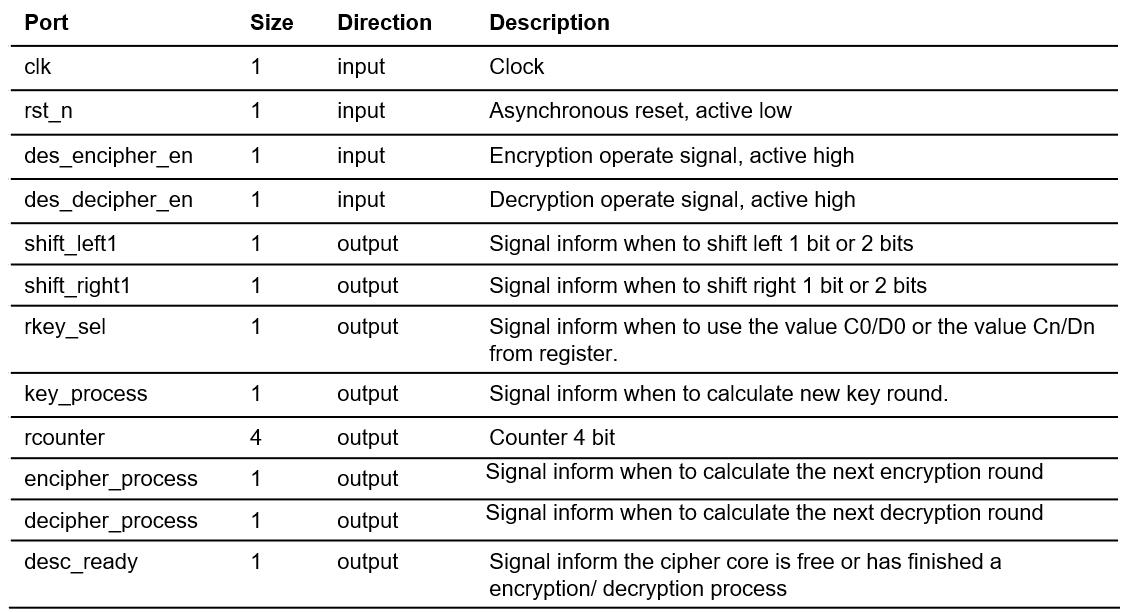


### **DES Controller:**

* Sơ đồ khối:



* Chức năng: Tạo ra các tín hiệu điều khiển cho các mạch được trình bày ở trên, bao gồm một bộ đếm và một bộ tạo tín hiệu để điều khiển chu kỳ khóa mới và thực thi vòng lặp tiếp theo.



* Waveform:

