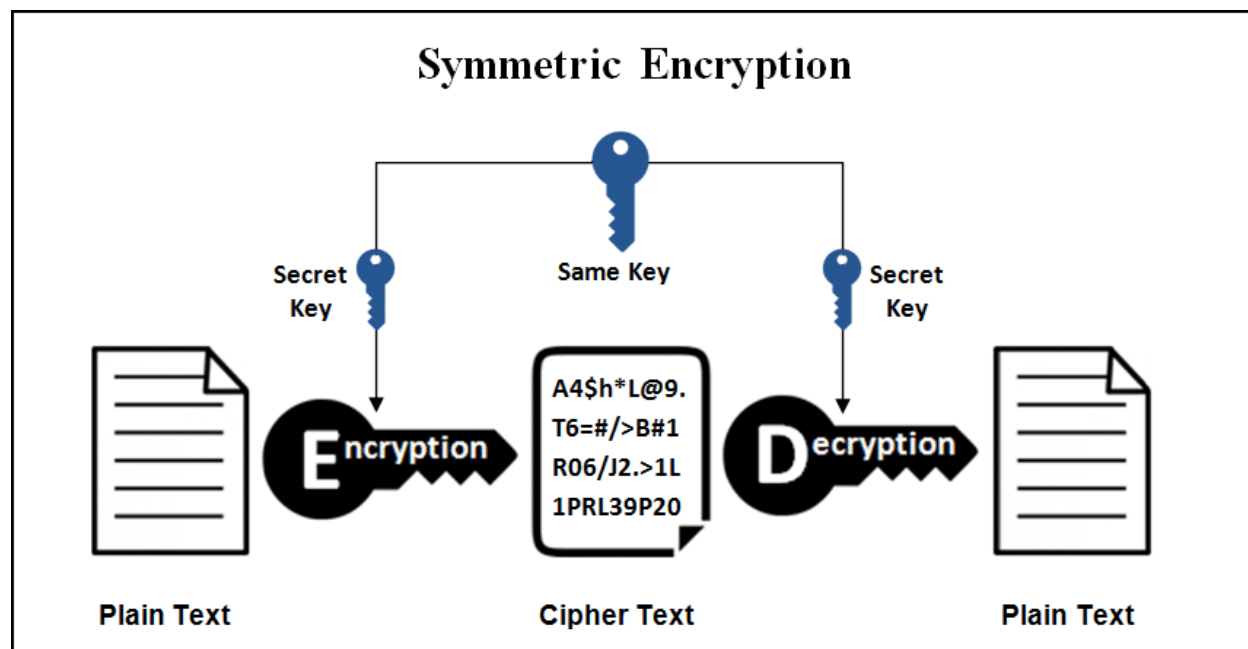


Digital Design Lab Project : Spring 98

Logic Encryption & Decryption Systems:

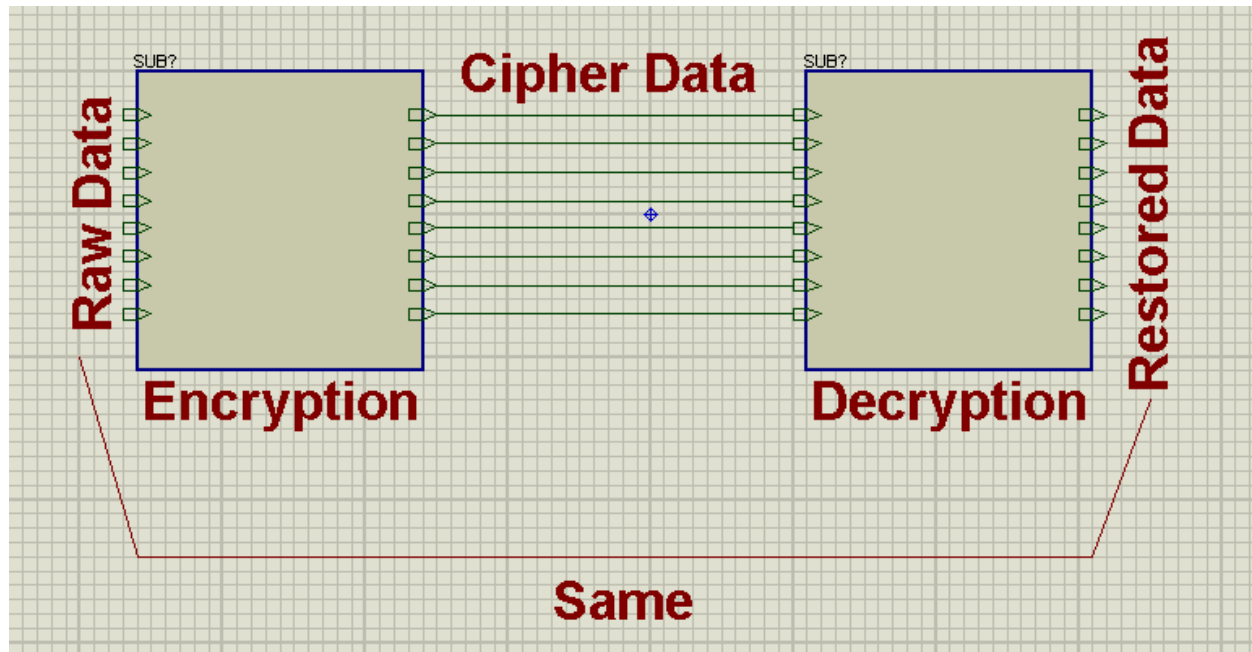
در اینجا **Encryption** به معنی قفل کردن (مخفی کردن) اطلاعات به وسیله یک کلید (**key**) است. بلاک مربوط به این فرایند یک عدد هشت بیتی را به عنوان ورودی میگیرد، ورودی دیگر این ماژول یک کلید هشت بیتی خواهد بود که ترکیب این دو رشته 8 بیتی به صورت **Combinational** یک خروجی تولید میکند. نکته اصلی غیر قابل شناسایی بودن ورودی **Data** اصلی از روی **Encrypted Data** است. کل فرایند مد نظر در شکل زیر مشخص شده است ، این حالت را برای اطلاعات متنی در نظر بگیرید :



همانطور که میبینید اطلاعات Encrypt شده به شکل نامفهوم هستند. و هر دو فرایند Encryption و Decryption به وسیله یک Key انجام میشوند.

فرایند Decryption را مشابه تابع معکوس برای تابع Encryption در نظر میگیریم.

برای یک مدار متشکل از Gate های منطقی یک مجموعه به شکل زیر خواهیم داشت:



که در اینجا حالت شبیه به حالت برای اطلاعات متنی را مشاهده میکنید.

یک روش ساده برای این فرایند این است که Encryption و Decryption هر دو با یک XOR انجام شوند که یک ورودی آن اطلاعات و ورودی دیگر کلید است.

حالت مد نظر برای انجام پروژه حالتی غیر از این (XOR) است. طراحی شما میتواند به هر شکلی انجام شود و تنها برقراری امنیت اطلاعات مد نظر است!

در اینجا نیاز به یک (برای هر داده) مژول تبدیل باینری به BCD خواهیم داشت که هر سه داده Raw Data و Cipher Data و Restored Data را در 7seg ها نمایش دهیم.

طراحی مورد نظر فقط عملکرد ذکر شده برای تغییر اطلاعات (غیر قابل تشخیص) و بازیابی آن است و الگوریتم خاصی مد نظر نیست و ترجیحا الگوریتم خودتان را پیاده سازی کنید (برای مثال از Truth Table یا تابع ابداعی خودتان استفاده کنید).