Preliminary Proposal Draft

ECE 337

Seth Bontrager
Anthony Kang
Eric Murphy
Isaac Sheeley

Thursday (11:30 - 2:20)

Due: 2/3/15

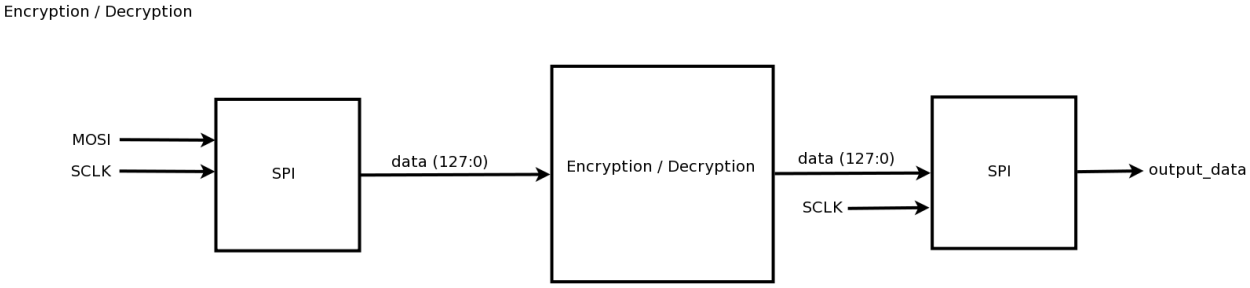
TA: Utpal Mahanta

Executive Summary

Our team wants to design and build a hardware implementation of the 3DES algorithm. The sending and receiving of encrypted data is an integral part of nearly all forms of commerce and internet communications. Our design of 3DES is important because many financial institutions still use the encryption standard, therefore developing a more efficient or faster implementation could be very beneficial. Our algorithm will be unique in the sense that we will be optimizing for speed of encryption and decryption. This will be accomplished by optimizing certain functional blocks at a gate level. The functional blocks of choice will be later determined by the estimated benefit of implementing them at a gate level. The 3DES algorithm is appropriate for ASIC because it's creators developed it will hardware implementation in mind. Because of this fact, 3DES can successfully be implemented in a hardware design to allow for the encryption and decryption of data without having to consume resources that a software based implementation would otherwise devour. In order to implement this design, we will need knowledge of the DES algorithm, a development and testing environment, work hours for developing and testing the design, and support from the course staff as we may encounter difficulties that are currently unforeseen. The remainder of this proposal goes over the details of implementing 3DES, such as the design specifications, a system usage diagram that shows a very high-level block diagram of the overall algorithm along with a diagram for one round of processing. It also details the operation characteristics that describes the functions that will be performed by our chip and identifies the general type of commercial part to which our final chip would be connected.

Design Specification

System Usage Diagram



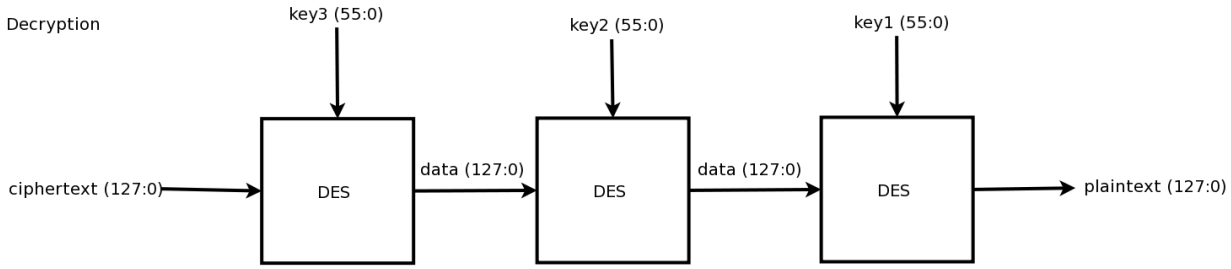
High Level Block:

This block encompasses the inputs, outputs, and the functionality of our design.

Port Descriptions:

Signal	Direction	Description
SCLK	input	The system clock, used to clock in values
MOSI	input	Data that is being clocked into the system (1 bit at a time)
output_data	output	Data is that being output (1 bit at a time)

Operational Characteristics



Encryption/Decryption Block

This is the block that implements each round of the algorithm.

Port Descriptions:

Signal	Direction	Description
clk	input	system clock signal with a 50% duty cycle
n_rst	input	Asynchronous active low system reset signal.
plaintext[127:0]	input/output	plaintext message for encrypted, decrypted message from decryption
ciphertext[127:0]	input/output	encrypted text input to be decrypted, encrypted text output from encryption
keys[0:3][0:55]	input	3 keys, one for each round of DES

DES Block

This block implements the 3 rounds of DES in triple DES

Signal	Direction	Description
plaintext[127:0]	input/output	left 32 bits of input block
ciphertext[127:0]	input/output	right 32 bits of input block
round_key[0:55]	input	round key used for encryption/decryption

Round Block

This is the block that houses the functional blocks for each step of the algorithm.

Port Descriptions:

Signal	Direction	Description
left[31:0]	input	left 32 bits of input block
right[31:0]	input	right 32 bits of input block
round_key[0:48]	input	round key used for encryption/decryption

Expand Block

Expansion block that uses a expansion permutation to expand 32 bits in to 48 bits.

Signal	Direction	Description
right[31:0]	input	right 32 bits of input block
data[47:0]	output	expanded 48 bits of input block

Substitution Block

Substitution block uses the expanded input block to substitute values from a lookup table.

Signal	Direction	Description
data[47:0]	input	expanded 48 bits
data_out[31:0]	output	substituted 32 bits

Permutation Block

Permutation block simply permutes the 32 bits using a preset permutation box

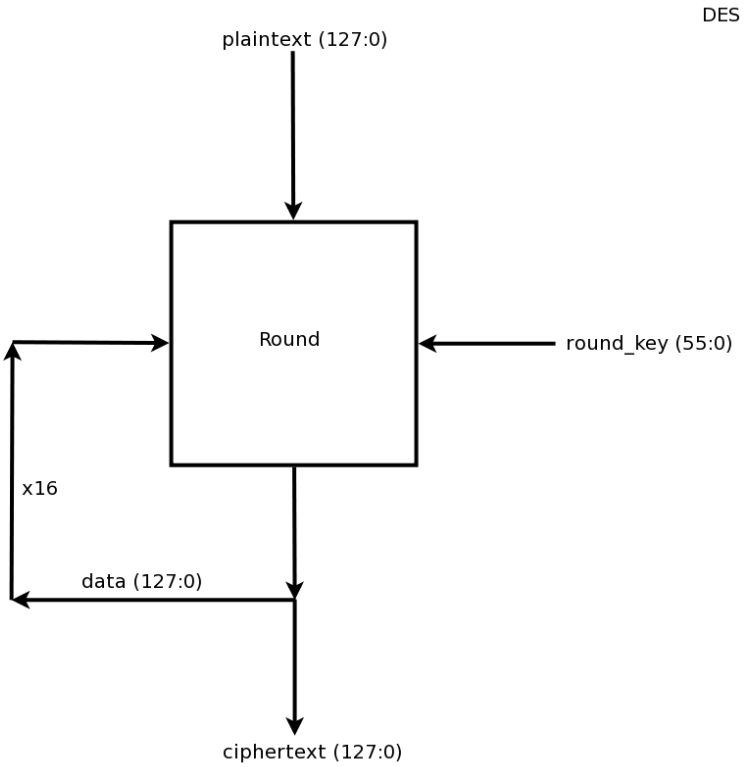
Signal	Direction	Description
data[31:0]	input	substituted 32 bits
data_out[31:0]	output	permutated 32 bits

KeyGen Block

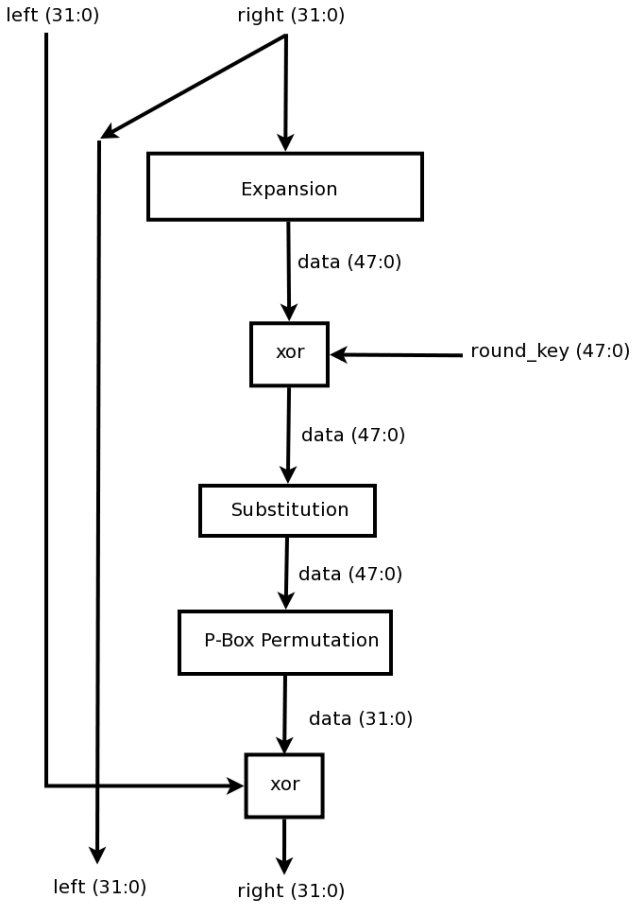
Key Generation block that generates the round key but doing a 56 bit permutation and a 48 bit contraction

Signal	Direction	Description
user_key[56:0]	input	user supplied 56 bit key
gen_enable	input	signals block to shift in user key
gen_next	input	signals the block to generate the next key
prev_key[56:0]	input	previous key, as next key depends on previous key

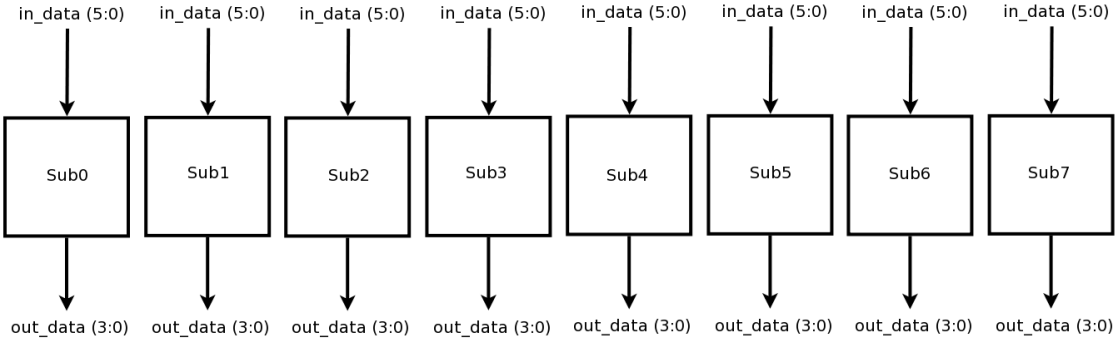
round_key[48:0]	output	48 bit permuted/contracted key



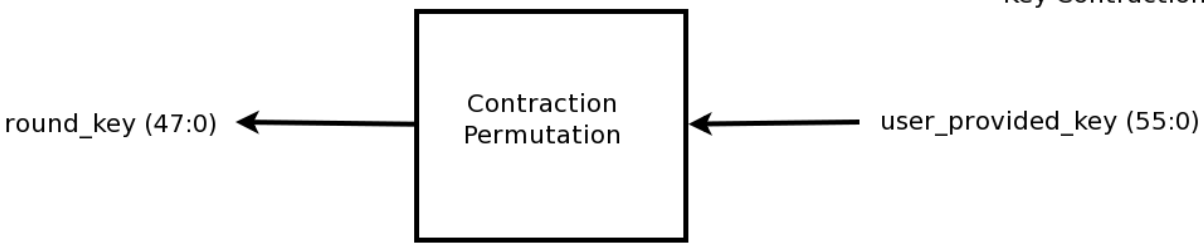
One Round of DES



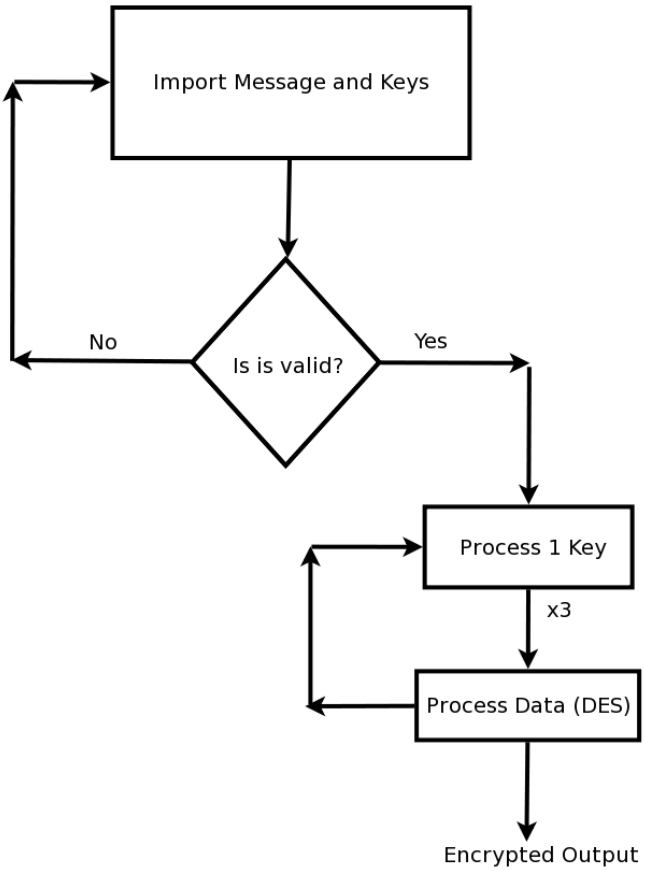
Substitution Step



Key Contraction



Flowchart of Chip Operation



Requirements

The use of Triple DES in encrypted network communication requires high speed to minimize the time it takes to encrypt the information and then decrypt it at the other end. The speed at which information can be sent is very critical in many industries today, and the methods used to encrypt the information must be fast in order to not create a bottleneck in the transmission of information. The primary optimization objective of our project will be to maximize speed. We will optimize the design for speed by implementing certain functional blocks at a gate level and performing certain task in parallel. Optimizing our design for area will be a secondary objective. Our target for the area will be the initial 1.5 mm x 1.5 mm for now until we get a better idea of the area required for our design. The pin count for our design will be 3 pins. Since data is going to be input and output in a serial manner, fewer pins are needed than in other kinds of designs.

Design Architecture

Encryption / Decryption