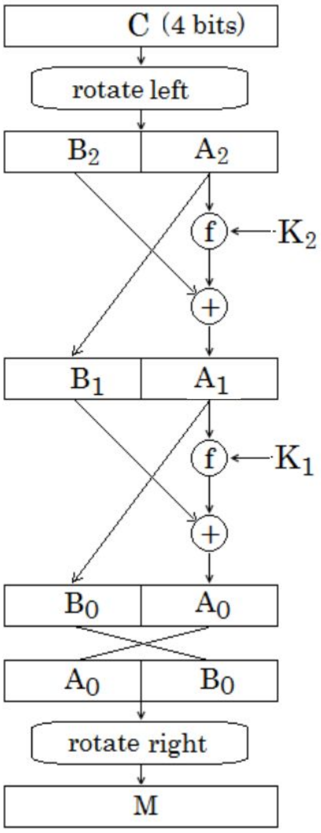
CSCI361 Assignment 2

Asjad Athick
4970512
mama158

Part 1: LDES

1. Decryption Diagram



2. Source code: ldes.cpp

3.

```
Key: 00 Value: 0000 Encrypted: 1001
Key: 00 Value: 0001 Encrypted: 1000
Key: 00 Value: 0010 Encrypted: 0011
Key: 00 Value: 0011 Encrypted: 0010
Key: 00 Value: 0100 Encrypted: 1100
Key: 00 Value: 0101 Encrypted: 1101
Key: 00 Value: 0110 Encrypted: 0110
Key: 00 Value: 0111 Encrypted: 0111
Key: 00 Value: 1000 Encrypted: 0001
Key: 00 Value: 1001 Encrypted: 0000
Key: 00 Value: 1010 Encrypted: 1011
Key: 00 Value: 1011 Encrypted: 1010
Key: 00 Value: 1100 Encrypted: 0100
Key: 00 Value: 1101 Encrypted: 0101
Key: 00 Value: 1110 Encrypted: 1110
Key: 00 Value: 1111 Encrypted: 1111
-----------------------------------
Key: 01 Value: 0000 Encrypted: 1111
Key: 01 Value: 0001 Encrypted: 1110
Key: 01 Value: 0010 Encrypted: 0101
Key: 01 Value: 0011 Encrypted: 0100
Key: 01 Value: 0100 Encrypted: 1010
Key: 01 Value: 0101 Encrypted: 1011
Key: 01 Value: 0110 Encrypted: 0000
Key: 01 Value: 0111 Encrypted: 0001
Key: 01 Value: 1000 Encrypted: 0111
Key: 01 Value: 1001 Encrypted: 0110
Key: 01 Value: 1010 Encrypted: 1101
Key: 01 Value: 1011 Encrypted: 1100
Key: 01 Value: 1100 Encrypted: 0010
Key: 01 Value: 1101 Encrypted: 0011
Key: 01 Value: 1110 Encrypted: 1000
Key: 01 Value: 1111 Encrypted: 1001
-----------------------------------
Key: 10 Value: 0000 Encrypted: 0110
Key: 10 Value: 0001 Encrypted: 0111
Key: 10 Value: 0010 Encrypted: 1100
Key: 10 Value: 0011 Encrypted: 1101
Key: 10 Value: 0100 Encrypted: 0011
Key: 10 Value: 0101 Encrypted: 0010
Key: 10 Value: 0110 Encrypted: 1001
Key: 10 Value: 0111 Encrypted: 1000
Key: 10 Value: 1000 Encrypted: 1110
Key: 10 Value: 1001 Encrypted: 1111
```

```
Key: 10 Value: 1010 Encrypted: 0100
Key: 10 Value: 1011 Encrypted: 0101
Key: 10 Value: 1100 Encrypted: 1011
Key: 10 Value: 1101 Encrypted: 1010
Key: 10 Value: 1110 Encrypted: 0001
Key: 10 Value: 1111 Encrypted: 0000
-----------------------------------
Key: 11 Value: 0000 Encrypted: 0000
Key: 11 Value: 0001 Encrypted: 0001
Key: 11 Value: 0010 Encrypted: 1010
Key: 11 Value: 0011 Encrypted: 1011
Key: 11 Value: 0100 Encrypted: 0101
Key: 11 Value: 0101 Encrypted: 0100
Key: 11 Value: 0110 Encrypted: 1111
Key: 11 Value: 0111 Encrypted: 1110
Key: 11 Value: 1000 Encrypted: 1000
Key: 11 Value: 1001 Encrypted: 1001
Key: 11 Value: 1010 Encrypted: 0010
Key: 11 Value: 1011 Encrypted: 0011
Key: 11 Value: 1100 Encrypted: 1101
Key: 11 Value: 1101 Encrypted: 1100
Key: 11 Value: 1110 Encrypted: 0111
Key: 11 Value: 1111 Encrypted: 0110
-----------------------------------
```

3.

```
Key = 00
E(0000) = 1001
E(0001) = 1000
E(0010) = 0011
E(0100) = 1100
E(1000) = 0001
```

Value to be encrypted	Function applied on components	Encrypted value

E(1100)	E(0000)
	E(1000)
	E(0100) XOR
		1001
		0001
		1100
		= 0100

E(1010)	E(0000)
	E(1000)
	E(0010) XOR
		1001
		0001
		0011
		=1011

E(1001)	E(0000)
	E(1000)
	E(0001) XOR
		1001
		0001
		1000
		=0000

E(0110)	E(0000)
	E(0100)
	E(0010) XOR
		1001
		1100
		0011
		=0110

E(0101)	E(0000)
	E(0100)
	E(0001) XOR
		1001
		1100
		1000
		=1101

E(0011)	E(0000)
	E(0010)
	E(0001) XOR
		1001
		0011
		1000
		=0010

E(0111)	E(0100)
	E(0010)
	E(0001) XOR
		1100
		0011
		1000
		=0111

E(1011)	E(1000)
	E(0010)
		0001
		0011

	E(0001) XOR	1000 =1010

E(1101)	E(1000)
	E(0100)
	E(0001) XOR
		0001
		1100
		1000
		=0101

E(1110)	E(1000)
	E(0100)
	E(0010) XOR
		0001
		1100
		0011
		=1110

E(1111)	E(0000)
	E(1000)
	E(0100)
	E(0010)
	E(0001) XOR
		1001
		0001
		1100
		0011
		1000
		=1111

The base components are added up to whatever value that needs to be encrypted. The relationship between the encrypted values of the base components and the result encrypted value is an XOR function (determined by function f).

Part 2: Mdes

4. mdes-v1.cpp

5.

```
Key: 00 Value: 0000 Encrypted: 0000
Key: 00 Value: 0001 Encrypted: 0100
Key: 00 Value: 0010 Encrypted: 1000
Key: 00 Value: 0011 Encrypted: 1100
Key: 00 Value: 0100 Encrypted: 0001
Key: 00 Value: 0101 Encrypted: 0101
Key: 00 Value: 0110 Encrypted: 1111
Key: 00 Value: 0111 Encrypted: 1011
Key: 00 Value: 1000 Encrypted: 0010
Key: 00 Value: 1001 Encrypted: 1001
Key: 00 Value: 1010 Encrypted: 1010
Key: 00 Value: 1011 Encrypted: 0111
Key: 00 Value: 1100 Encrypted: 0011
Key: 00 Value: 1101 Encrypted: 1110
Key: 00 Value: 1110 Encrypted: 1101
Key: 00 Value: 1111 Encrypted: 0110
----------------------------------
Key: 01 Value: 0000 Encrypted: 0110
Key: 01 Value: 0001 Encrypted: 0010
Key: 01 Value: 0010 Encrypted: 1000
Key: 01 Value: 0011 Encrypted: 1100
Key: 01 Value: 0100 Encrypted: 0001
Key: 01 Value: 0101 Encrypted: 0101
Key: 01 Value: 0110 Encrypted: 1001
Key: 01 Value: 0111 Encrypted: 1101
Key: 01 Value: 1000 Encrypted: 0100
Key: 01 Value: 1001 Encrypted: 1111
Key: 01 Value: 1010 Encrypted: 1010
Key: 01 Value: 1011 Encrypted: 0111
Key: 01 Value: 1100 Encrypted: 0011
Key: 01 Value: 1101 Encrypted: 1110
Key: 01 Value: 1110 Encrypted: 1011
Key: 01 Value: 1111 Encrypted: 0000
----------------------------------
Key: 10 Value: 0000 Encrypted: 1111
Key: 10 Value: 0001 Encrypted: 0100
Key: 10 Value: 0010 Encrypted: 0001
```

```
Key: 10 Value: 0011 Encrypted: 1100
Key: 10 Value: 0100 Encrypted: 1000
Key: 10 Value: 0101 Encrypted: 0101
Key: 10 Value: 0110 Encrypted: 0000
Key: 10 Value: 0111 Encrypted: 1011
Key: 10 Value: 1000 Encrypted: 0010
Key: 10 Value: 1001 Encrypted: 0110
Key: 10 Value: 1010 Encrypted: 1010
Key: 10 Value: 1011 Encrypted: 1110
Key: 10 Value: 1100 Encrypted: 0011
Key: 10 Value: 1101 Encrypted: 0111
Key: 10 Value: 1110 Encrypted: 1101
Key: 10 Value: 1111 Encrypted: 1001
----------------------------------
Key: 11 Value: 0000 Encrypted: 1001
Key: 11 Value: 0001 Encrypted: 0010
Key: 11 Value: 0010 Encrypted: 0001
Key: 11 Value: 0011 Encrypted: 1100
Key: 11 Value: 0100 Encrypted: 1000
Key: 11 Value: 0101 Encrypted: 0101
Key: 11 Value: 0110 Encrypted: 0110
Key: 11 Value: 0111 Encrypted: 1101
Key: 11 Value: 1000 Encrypted: 0100
Key: 11 Value: 1001 Encrypted: 0000
Key: 11 Value: 1010 Encrypted: 1010
Key: 11 Value: 1011 Encrypted: 1110
Key: 11 Value: 1100 Encrypted: 0011
Key: 11 Value: 1101 Encrypted: 0111
Key: 11 Value: 1110 Encrypted: 1011
Key: 11 Value: 1111 Encrypted: 1111
----------------------------------
```

Verify the linear relationship doesn’t exist when using an s-box

Key 11

Base components	Expected result if linear	Result using s-box
E(0000) = 1001 E(0001) = 0010 E(0010) = 0001	E(0011) should be 1010 if linear	The actual result as showed in the output above is 1100

This shows the relationship is not linear if an s-box is used

6. Source code: mdes.cpp