Implementation of the Data Encryption Algorithm in Matlab

# Introduction

Data Encryption Standard was the first cryptographic standard that was developed by IBM and the NSA. It is a block cipher that operates on 64 bit blocks. The algorithm consists of a round in which there are substitutions and permutations which encrypt the plaintext. It uses a 56 bit key to encipher the plaintext. Each block undergoes 16 rounds, thereafter it is considered ciphertext. The Data Encryption Algorithm contains within it, an algorithm to determine a subkey for each round.

# Method

## Initial Permutation

The data undergoes an initial permutation, this is merely a transposition of the 64 bit plaintext.

## Subkey Algorithm

The input to the Subkey Algorithm consists of a 64 bit key. This key contains parity bits for security. Bits are selected from the 64 bit key to create a new 56 bit key, removing the parity bits. The new key is thereafter used to create 16 subkeys. This is done by dividing the key into two parts(left and right). The right and the left parts are circularly shifted left by a value that is determined by the index of the round. The left and right part is combined again and is compressed to create a 48 bit subkey for that particular round.

## Algorithm for a single round

The input for a round consists of the 64 bit plaintext and a subkey for that particular round. The plaintext is split into two parts(left and right).

### Expansion Permutation

The right part of the input is then expanded using an expansion permutation. The expansion maps a single bit from the input to multiple bits in the output. The right part now is expanded from 32 bit to 48 bits.

### Exclusive OR

The expanded part is then exclusive ORed (EXOR) with the subkey for that particular round.

### SBox

The SBox is a substitution cipher. It takes the result of the EXOR(48 bits), and splits it into eight vectors of six digits(8x6). It combines the first and last bit of the 6 digit vector to form a binary number which is used as a reference for the row. The middle 4 bits are used to create a binary number that will reference the column. The number situated in the position of the row and column is used as the output. The number is a four bit number. This changes the 48 bit input into a 32 bit output.

### PBox

This is a direct transposition of the 32 bits.

The left part of the plaintext is XORed with the result of the PBox, and this becomes the new right part. The initial right of the input becomes the new left.

The process of the round is repeated 16 times for every single 64 bit block of plaintext.

# Cryptanalysis

## Strengths

### SBox

The SBox is the greatest strength of the encryption. This is not a transposition and this defends against a brute force attack.

### Expansion Permutation

The Expansion Permutation maps one input to multiple outputs. This allows the input bits to spread faster to the output

## Weaknesses

### Weak Keys

Weak encryption keys generates the same subkey for all 16 rounds. This reduces the security of the encryption. There are three levels of weak keys: Weak Keys, Semiweak Keys and Possibly Weak Keys

### Short Key Length

The length of the key is 64 bits. The small key length decreases the security of the encryption against a brute force attack.

## Brute Force

In 1997, Deschall Project won a contest to break the DES. In 1998, Electronic Frontier Foundation created a machine to break the DES. Lastly in 2006, the University of Bochum created the Copacabana machine to break the encryption.

## Davies attack

An attack specialised to the DES was created by Donald Davies. It requires 2^50 known plaintexts.

## Differential Cryptanalysis

It requires 2^47 known plaintexts and is more efficient than a Davies effect.

## Linear Cryptanalysis

It requires 2^43 known plaintexts and is the most efficient method to break the encryption.

## Secure Encryption

### Triple Des

This applies the DEA three times on each block of plaintext. The result is 168(3x56) independent keys. This defends against cryptanalysis techniques

### AES

The DES was followed by a stronger encryption in 1998. The key size is greater than 128 bits which is stronger and more resistant to attacks.

# Conclusion

The data encryption algorithm is not a secure algorithm as there are many ways to break the algorithm. It is a relatively primitive algorithm and has been superseded by stronger algorithms with longer key lengths that are more resistant to attacks.