DES- Data Encryption Standard

Indumathi Saikumar

Post Graduate Student, Electronic and Communication Engineering,
CMR College of Engineering and Technology, Telangana, India

Abstract - *The data encryption standard is also known as DES.DES has been the most extensively used encryption algorithm standard in recent times. Encryption and decryption comprise of cryptography. Cryptography terminology is used in the data encryption standard along with standard algorithm to hide the original text. DES applies the cipher algorithm to each data block. Data encryption is being used to hide the true meaning of data so that it is very hard to attack or crack. This paper deals with the simulation and synthesis results of implemented DES algorithm. Analysis of implementation is shown in step by step process. A test case is analyzed step by step to check the results at each step of the algorithm.*

Key Words: *DES, Cryptography, Encryption, Decryption*

1. INTRODUCTION

Data which can be read and understood without any special measures is called as plaintext. Disguising plaintext in such a way to hide its true meaning is called encryption. Encrypting plaintext results in unreadable gibberish form called cipher text. Encryption is done to hide the data from anyone for whom it is not intended. Reverting the cipher text to its original plaintext is called as decryption. DES method is used to store sensitive information or transmit information across insecure networks so that it cannot be read by anyone except the intended recipient.

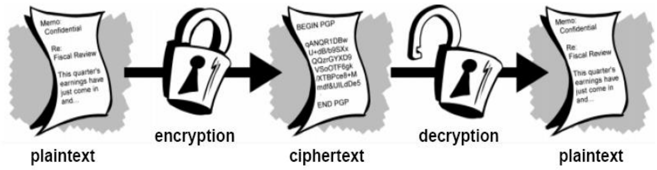


Fig -1: Encryption and decryption

Data encryption standard uses cryptographic algorithm that can be used to protect electronic data. There are three methods of encryption standard they are symmetric cryptography, asymmetric cryptography and hash function. DES algorithm makes use of symmetric cryptograph. Block cipher algorithm is used for encryption and decryption purpose and the message is divided into blocks of bits. DES processes the input data (Original message) of block size 64-bits and a secret key of 64-bits to provide a 64-bit cipher text.

2. CRYPTOGRAPHY

Cryptography is derived from Greek language kryptos means hidden and grafos meaning write or speak which means study of hiding information. It is the science of securing data. Cryptography is a science of using mathematics to encrypt and decrypt data. Cryptography enables to store important data or transmit it across insecure networks so that it cannot be read by anyone except the intended recipient. Cryptography examples include the security of the ATM cards, computer passwords and electronic commerce which all depend upon cryptography.

2.1 Purpose of cryptography

Cryptography is necessary when communicating over any medium such as internet. Mostly used for communicating over un-trusted medium. To send information over an untrusted medium there are some specific requirements such as

Authentication: Authentication is a process of identifying an individual, such as based on username and password.

Privacy: Privacy is ensuring the sender that the message can be read by the intended receiver and no one else.

Integrity: Assuring the receiver that the received message has to been altered in any way from the original.

Non-repudiation: It is a method of guaranteeing message transmission between two parties. Successful completion of message sent and received.

3. METHODS OF ENCRYPTION

There are several blocks in an encryption method, the two main blocks are the algorithms and the key. Algorithms are the complex mathematical formulas that dictate the rules of how the plaintext will be converted into cipher text. Key is a set of random bits that will be inserted into the algorithm. Two users can communicate via encryption, they must use the same algorithm and the same key. In some encryption cases, the receiver and sender use the same key and in other encryption cases they must use different keys for encryption and decryption process. There are three different methods of encryption namely symmetric asymmetric and hash function method for encryption and decryption.

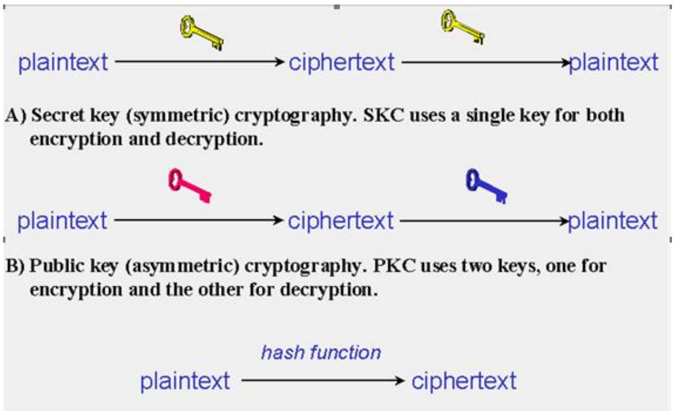

plaintext
ciphertext
plaintext
A) Secret key (symmetric) cryptography. SKC uses a single key for both encryption and decryption.
plaintext
ciphertext
plaintext
B) Public key (asymmetric) cryptography. PKC uses two keys, one for encryption and the other for decryption.
hash function
plaintext
ciphertext

Fig -2: Two types of cryptographic algorithms

Cryptography algorithms use either symmetric keys or asymmetric keys. Symmetric keys are also called secret keys which uses a single key for encryption and decryption. Asymmetric keys are also called as public keys which makes use of two different keys for encryption and decryption.

3.1 Symmetric cryptography

In symmetric cryptography both the parties i.e. the sender and the receiver will be using the same key for encryption and decryption process as show in Figure 2.

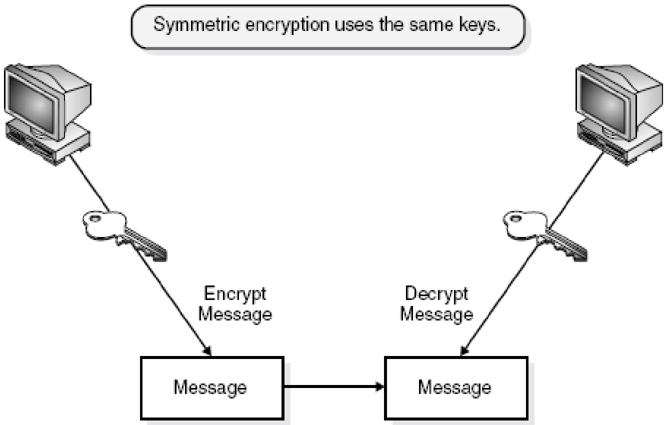


Fig -3: Symmetric algorithms, both the sender and receiver use the same keys to encryption and decryption message

A sender uses a key to encrypt plain text into cipher text and sends it to the receiver. Receiver uses the same key to decrypt the cipher text into plain text. As told above symmetric key is also called as secret key, because this type of encryption depends on each user, there can be more than one user but the users should keep the key a secret and properly protect it. If this key goes into the intruder's hand, that intruder has the access to decrypt any intercepted message encrypted with this key. Some type of symmetric algorithms are DES, Triple DES, AES and etc.

The following list outlines the advantages and disadvantages of symmetric key systems:
Advantages:

1. Much faster than asymmetric method
2. Hard to break the key if large key size is used
3. Compared to asymmetric systems, symmetric algorithms scream in speed.

Disadvantages:

1. Key distribution. The key must be delivered in a proper way.
2. Scalability
3. Limited security

3.2 Asymmetric cryptography

In asymmetric cryptography two different keys are used for encryption and decryption. In this type of cryptography a pair of key is made up of one public key which can be known to everyone and one private key which is known only to the owner. Example of asymmetric cryptography is demonstrated for better understanding.

A
Lockbox
Password
30293014
A
A

Fig -4: A represents Alice's lock, Lockbox, key, Safe Locker, Encrypted message

Alice has a password for her safe locker and keeps key safely in the locker. Lock is available to everyone. Lock is kept in the lockbox. Alice friends bob, peter, mike can send her private messages. To do that they need copies of Alice's lock. Alice sends them copies of her lock, and they put them in their lockboxes. Her friends can now send private message with Alice's lock and sends it to her. When Alice receives her email she opens the safe locker with her password takes the key out and unlocks the email. In the same way Alice can send message to Bob, peter, mike. Alice encrypts a message with Bob's lock and sends it to Bob. Bob uses his key to unlock the message.

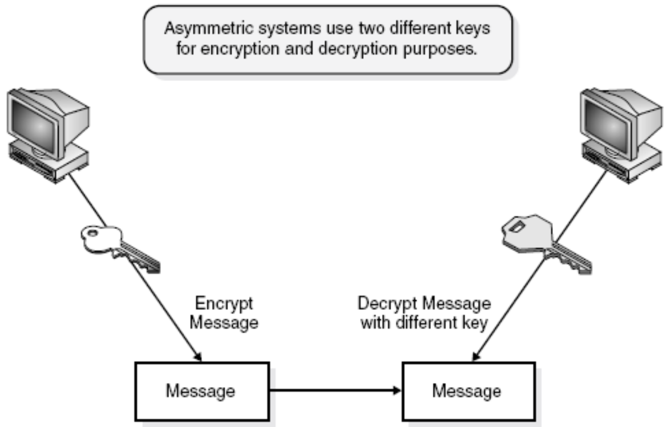

Asymmetric systems use two different keys for encryption and decryption purposes.
Encrypt Message
Decrypt Message with different key
Message
Message

Fig -5: Symmetric algorithms, both the sender and receiver use the same keys to encryption and decryption message

The following outlines the strengths and weaknesses of asymmetric key systems: Strengths, Better key distribution than symmetric systems, Better scalability than symmetric systems, Can provide confidentiality, authentication, and non-repudiation, Weaknesses, Works much slower than symmetric systems.

The following are examples of asymmetric key algorithms:

- RSA
- Elliptic Curve Cryptosystem (ECC)
- Diffie-Hellman
- El Gamal
- Digital Signature Standard (DSS)

4. DES

The Data Encryption standard is used to protect electronic data. DES algorithm uses symmetric block cipher for encrypting and decrypting data. Encryption converts data into gibberish language called cipher text. Decrypting the cipher text gives us back the original data that is plaintext. Converting the information from cipher to plain we use a standard form of algorithm called Symmetric algorithm.

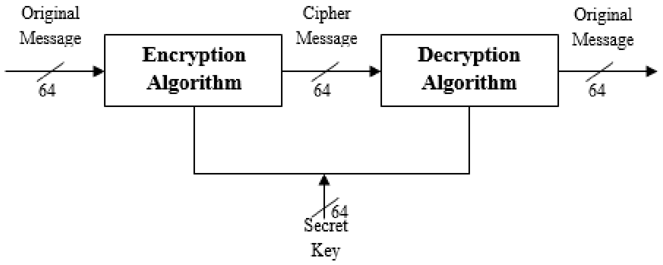


Fig -6: Overall Representation of Encryption and decryption

DES takes an input of 64bits and the output is also of the same size. The process requires a second input, which is a secret key with length of 64bits. Block cipher algorithm is used where message is divided into blocks of bits. Block cipher is used for encryption and decryption. These blocks of bits are put through substitution, transposition, and other different mathematical functions.

Advantages of DES

- By using DES, input message of 64bits can be encrypted using the secret key length of 64bits.
- The encrypted key is cipher key which is expanded into a larger key, which is later used for other operations
- DES is hard to attack
- DES is very hard to crack because of the number of rounds used in encrypting message.
- DES is faster when compared RSA Encryption Algorithm.

DES has high level of security. It is completely specified and very easy to understand. It is adaptable to different applications. Data rates are high. DES can be validated and Exportable.

4.1 DES Application

- DES algorithm was made mandatory for all financial transactions by the U.S government which involves electronic fund transfer.
- High speed in ATM
- It is used for secure video teleconferencing
- Used in Routers and Remote Access Servers
- It can be used by federal departments and agencies when they require cryptographic protection for sensitive information.

5. DATA ENCRYPTION STANDARD ALGORITHM

Data Encryption Standard means to encrypt plaintext on the basis of standard that was developed. There is some critical data used for encryption and decryption know as a key. The algorithm used to encrypt data is a standard algorithm. Using standard algorithm data can encrypted and decrypted.

Table1. Description of DES algorithm Blocks

IP	Initial Permutation
IP^{-1}	Inverse Permutation
PC_1	Permuted Choice-1
PC_2	Permuted Choice-2
E	Expansion Permutation
P	Permutation

The above mentioned functions are carried out for every individual round. Based on the key provided a new key will be generated in the key schedule block. The new key is given as input to each round. There are four types

1. Permutation
2. Shifting
3. Substitution Box (S-box)
4. Instantiations

As per the standard, input 64 bits is taken, Initial permutation will be performed after which the 16 rounds with the input 64 bits key length is performed and finally the result of the last round will be given to Inverse Permutation. All the blocks perform operation separately.

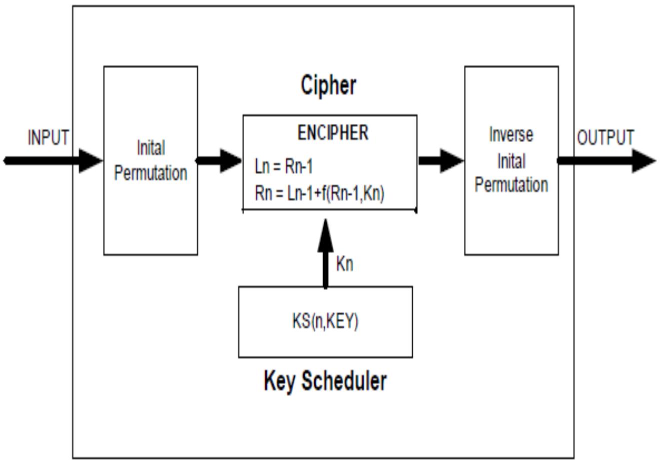


Fig -7: Top Level Block diagram of DES Algorithm

The above Figure.7 shows top level block diagram of DES algorithm.

6. ENCRYPTION

DES intakes input data of block size 64 bits and 64 bit key to provide a 64 bit cipher text. In the 64 bit key, every eighth bit is used as parity checking bit. So, 56 bits takes part in the algorithm to encrypt data. The 64 bit data is sent to “initial permutation” which provides 64 bit output. The 64 bit key is being fed to “permutation choice1” (PC_1). The output of PC_1 is 56 bits by ignoring the bit with sequence number in multiples of 8. The two outputs of PC_1 are fed to the first round in the sequence of 16 round blocks.

The round block divides its input into two equal parts, the data bits have parts L_i of 32 bits and R_i of 32 bits.

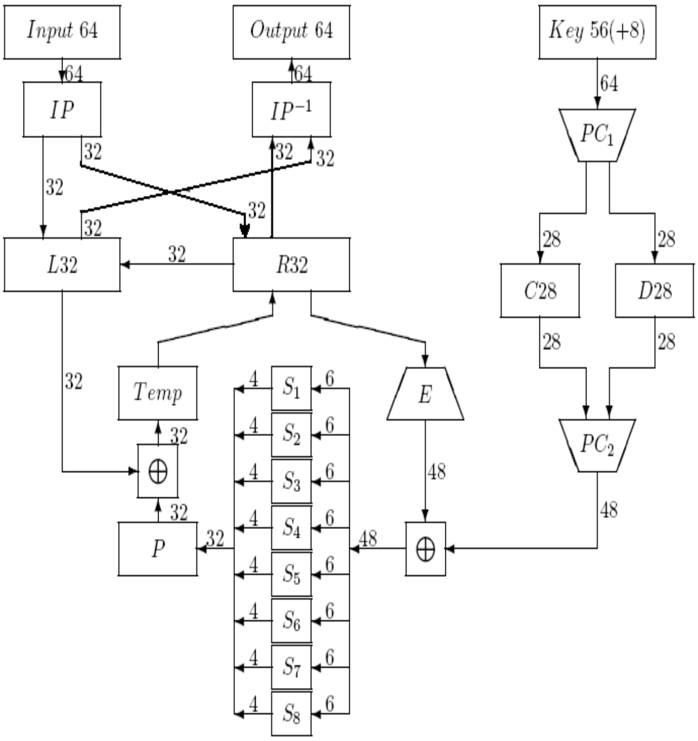


Fig -8: DES Algorithm blocks

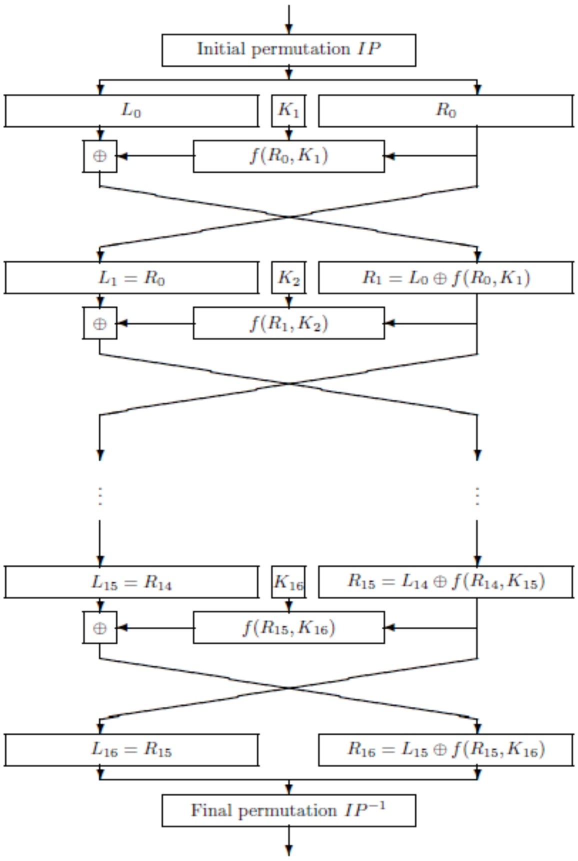


Fig -9: DES Algorithm with 16 Rounds

Similarly, key bits are divided in two parts C_i and D_i each of 28 bits of length. The 56 bits are used to generate the 48 bit round key through the "permutation chooice2". The 32 bit round key R_i is expanded to 48 bit round key through 'expansion permutation'. The output from PC_2 block is XOR-Ed with expansion permutation block to get the 48 bit address for the substitution box (S-box). The 48 bits is given as sequence to S-box into 8 sections, each of 6 bits. The S-box replaces every 6 bit of data to 4 bit data. The 32 bits from S-box is sent to the 'permutation function' to provide more diffusion of bits. "Permutation function" bits are XOR-Ed with the 32-bit L_i. This output of XOR is connected to the R_i of the next round. L_i of the next round is connected to R_i of this round. The output from L_i of 32 bits and R_i 32 bits is feed to the 'Inverse Permutation'. Output of 64 bits is obtained from IP^{-1}. C_0 and D_0 are connected to C_i and D_i of the next round. Out of 16 rounds of operation, 12 rounds have 2 left circular shifts and the rest 4 have only 1. The 64 data bits from the round 16 are operated with 32 bit swap and then fed to the IP^{-1}. In the Final stage of the encryption it provides another transposition before getting the final 64 bit sequence called Cipher text.

All the rounds of operation are clearly represented in the figure.8 and figure.9 and also the Algorithm is clearly explained. All the operations such as initial permutation, inverse permutation, substitution box, expansion permutation, key schedule for the key generation are carried with respect to the pre-defined standard tables.

7. ANALSIS OF THE IMPLMENTATION

The DES algorithm can be implemented using the Verilog HDL code. A test case is analyzed step by step to check the results at each step of the algorithm.

Input data=$0123456789ABCDEF_H$

Encryption key=$133457799BBCDFF1_H$

$0123456789ABCDEF_H \xrightarrow{\textit{Initial Permutation}} CC00CCFFF0AAF0AA_H$

$133457799BBCDFF1_H \xrightarrow{\textit{Permutation Choice1}} F0CCAAF556678F_H$

Round 1 Inputs, Operation and Outputs

Inputs: L_i=$CC00CCFF_H$

R_i=$F0AAF0AA_H$

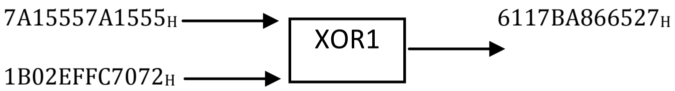
C_i=$F0CCAAF_H$ & D_i=$556678F_H$

$F0CCAAF_H \xrightarrow{\textit{Left Circular Shift (for C)}} E19955F_H$

$556678F_H \xrightarrow{\textit{Left Circular Shift (for D)}} AACCF1E_H$

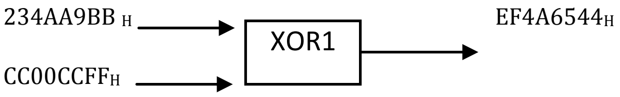
$556678FAACCF1E_H \xrightarrow{\textit{Permutation Choice2}} 1B02EFFC7072_H$

$F0AAF0AA_H \xrightarrow{\textit{Expansion Permutation}} 7A15557A1555_H$



$6117BA866527_H \xrightarrow{\textit{Substitution Box}} 5C82B597_H$

$5C82B597_H \xrightarrow{\textit{Permutation Function}} 234AA9BB_H$



Outputs: L_o=$F0AAF0AA_H$

R_o=$EF4A6544_H$

C_o=$E19955F_H$ & D_o=$AACCF1E_H$

The outputs of round 1 is given as inputs to the round 2 to its respective ports.

After 16 rounds of operation the final outputs are

L_o= 43423234_H,

R_o= $0A4CD995_H$,

C_o=$F0CCAAF_H$ and D_o=$556678F_H$

The values of C and D return to the initial values after completion of 16 rounds. The last stage is the inverse permutation to get the final result.

$0A4CD99543423234_H \xrightarrow{IP^{-1}} 85E813540F0AB405_H$

Finally, we receive the cipher text.

Cipher text= 85E813540F0AB405$_H$

Therefore when 64 bit input data and 64 bit key data is given 16 rounds of operations are performed with the standard algorithm we get a 64 bit output that is a cipher text. This is called encryption. In the same way with the same key the data can be decrypted. The coding for DES algorithm in Verilog HDL and implementation of the logic on FPGA can provide the knowledge about the operations taking place in DES to encrypt data.

3. CONCLUSION

The concept of cryptography long with encryption and decryption is explained. DES has 16 rounds of operation. The plaintext is taken to 16 rounds of operation which produces a cipher text. With the same key and data any implementation it produces same output as the algorithm specified in this standard. Data Encryption Standard has increased the level of security because of the 16 rounds of operation. It is difficult for the unauthorized party to attack and crack. s

REFERENCES

[1] Applied Cryptography: Protocols, Algorithms, and Source Code in C, by Bruce Schneier.

[2] Understanding Cryptography: A Textbook for students and Practitioners by christof Paar, Jan Pelzl , Bart Preneel

[3] Public-Key Cryptography Arto Salomaa, second edition, Springer, 1996. ISBN 3-540-61356-0.

[4] http://faculty.nps.edu/dedennin/publications/DES-15Years.pdf

[5] http://csrc.nist.gov/groups/ST/toolkit/block_ciphers.html

[6] http://faculty.nps.edu/dedennin/publications/DES-15Years.pdf

[7] https://en.wikibooks.org/wiki/Cryptography/DES

[8] http://csrc.nist.gov/publications/PubsSPs.html#800-131A