Comparison of AES and DES Algorithm

Shruti Kumari*
Gautam Kumar**

Abstract

Cryptography is used for protection of information security. There are various algorithms like DES, RSA, HASH, MD5, AES, SHA-1 and HMAC.DES algorithm is developed by IBM. This algorithm used a 56 bit key to encipher/decipher a 64 bit block of data.In this paper we will compare between DES and RSA algorithm .In ATM DES algorithm is used in live at some place but AES algorithm should be used everywhere, we will also show how AES is better in ATM.

Keywords: Cryptosystem,Encipher, Decipher.

Introduction

Encryption is the process of encoding the plaintext into cipher text and Decryption is the process of decoding cipher text to plaintext. There are two types of encryption and decryption technique symmetric key cryptography and asymmetric key cryptography .In symmetric key cryptography sender and receiver both use same key,But in asymmetric key cryptography sender and receiver both uses different key. Symmetric key cryptography includes DES, AES, 3DES, IDEA, Blowfish algorithm etc. ,and asymmetric key cryptography includes RSA algorithms[1].

AES ALGORITHM

AES is created by the National Institute of Standards and Technology (NIST).The algorithm has been developed to replace the Data Encryption Standard (DES).AES is more secure than DES.AES is six times faster Than DES [2].The algorithm uses three rounds -10,12 or 14.The size are 128,192 or 256 bits according to the number of rounds. Several rounds made of several stages. This algorithm is used to encrypt electronic data.AES is adopted by US but now it is used by whole world. It is a symmetric key algorithm; same key is used for encryption and decryption.

On May 26, 2002 AES became effective as a federal government standard after approved by the Secretary of Commerce. AES is found in some other encryption package. [3]

DES ALGORITHM

Data Encryption Standard (DES) is a symmetric key, developed by IBM This algorithm uses a 56-bit key to encrypt/decrypt 64-bit data. The algorithm is best for

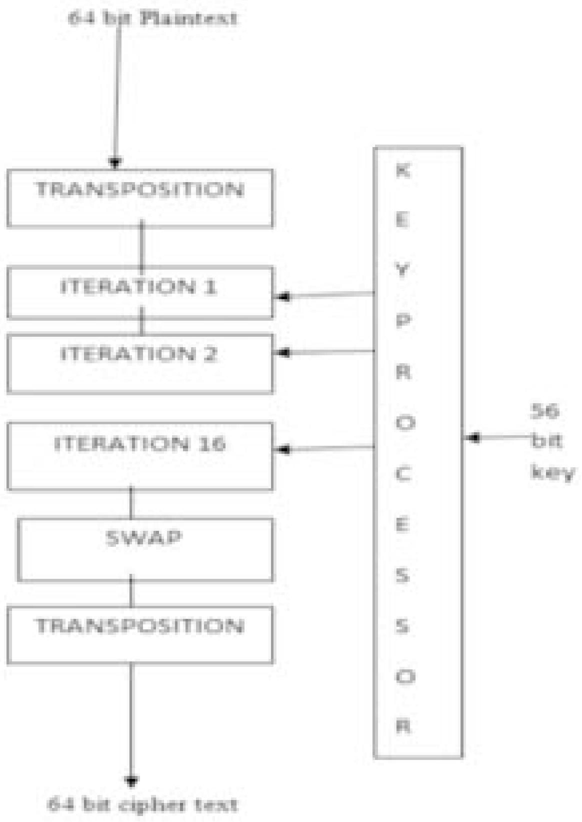

Figure-1.Encryption/Decryption Technique in DES

Shruti Kumari*
MCA (4th) M.E.R.I. (GGSIPU)

Gautam Kumar**
MCA (4th) M.E.R.I. (GGSIPU)

hardware. Key length is too short[4].The key is put through 19 different and complete procedures to create a 64-bit ciphertext.DES has two transposition block and 16 complex blocks called iteration blocks[5].

COMPARISON OF DES AND AES

DES is developed in 1977 and AES is developed in 2000.Key size of DES is 56-bit but key size of AE is 128,192,256 bits. Block size of data in DES is 64-bit but in AES is 128-bits.Both are symmetric key algorithm. Speed of encryption/decryption is moderate in DES but faster in AES.Power consumption is low in both. DES is not secureenough and AES excellent secured. Same key is used for encryption and decryption in both. Simulated speed is faster in both[6].

How DES Works in ATM

ATM uses secret key ,called the PIN key ,to derive the PIN from the account number in terms of algorithm known as DES.The result is natural PIN ,an offset can be added to it and then final PIN which the customer enter. The offset has no cryptographic function, it just used for customer to choose their own PIN [7].

EXAMPLE:
Account number: 6693082465987012
PIN key:FEFEFEFEFEFEFEFE
Result of DES:B6AE897C54ECD43A
Result decimalized:0665148956702468
Natural PIN:0664
Offset:4646
Customer PIN:5678

Usually DES is use to encrypt the ATM transaction but most of time need more secure triple DES.There are many illegal withdrawals take place from ATM.RossAnderson,a researcher investigated various cases of illegal withdrawals and exposing errors in bank security. There have many cases in which criminals used fake machines, attached keypads or card readers to real machines, and record customer's PIN and bank account details to access the accounts illegally. The algorithm selected as an Official Information Processing Standard (FIPS) for the United States. There are four different mode of operation, these four modes are Electronic Codebook (ECB) mode, the Cipher Block Chaining (CBC) mode, the Cipher Feedback (CFB) mode and the Output Feedback (OFB) mode.ECB is used for direct application in DES to encrypt/decrypt.CBC is modified form of ECB.CFB uses previous cipher text as an input totheDES to produce output which combined with plaintext ,OFB is same as CFB but in OFB previous output of DES is used as input.

Program for encrypting and decrypting with DES

```
#include"msp 430xxxx.h"
#include"TI_DES.h"
Intmain(void)
{
Des_ctx dc1;
Unsigned char *cp;
Unsigned char
data[]={0x24,0xc2,0xa0,0xe7,0x5b,0x6a,0xa3,0x50};
Unsigned char key
[8]={0x01,0x15,0x24,0x07,0x17,0x15,0x26,0x18};
Cp=data;
De_key(&dc1,key,ENDE);
DE_En(&dc,cp,1);
DE_De(&dc,cp,1);
Return 0;
}
```

How AES is used in ATM

ATM using DES has been breached 24 hours. Advanced encryption standard (AES)is recent and new encryption algorithm.AES support AES with CBC (cipher block chaining) mode to IP security .[9]

Program of Encrypting with AES

```
#include "msp 430xxxx.h"
#include "TI_aes.h"
Intmain(void)
{
Unsignedcharstate[]={0x64,0x72,0x90,0xb2,0x22,
0x72,0xa1,0xb6,0xC5,0x5a,0x49,0x28,0x44,0xa0,
0xC2,0x01};
UnsignedcharKey[]={0x12,0x06,0x01,0x43,0x72,
0x15,0x15,0x91,0x52,0x21,0x31,0x71,0x26,0x38,
0x45,0x81};
Ae_en_de(state,key,0);
Return 0;
}
```

Program of Decrypting with AES

```
#include "msp 430xxxx.h"
#include "TI_aes.h"
Int main (void)
Unsignedcharstate[]={0x69,0x45,0x87,0x61,0x56,
0x87,0x23,0x54,0x34,0x21,0x41,0x73,0x91,0x61,
0x95,0x14};
Unsignedcharkey[]={0x00,0x11,0x12,0x13,0x14,
0x15,0x16,0x17,0x18,0x19,0x22,0x21,0x24,0x41,
0x32,0x64};
Ae_en_de(state,key,1);
Return0;
```

Conclusions

Encryption algorithm is very important in communication because it provides security.This paper based on AES and DES cryptographic algorithm technique, how DES at some place used in ATM and AES is more secure than DES so at everywhere in ATM AES algorithm should be used.

Acknowledgement

I would like to thank my faculty, college staff for their abundance guidance and support. Without their cooperation & motivation this research paper won't be possible.

References

1. www.scholar.google.co.in/21-01-2015/7:00pm
2. www.scholar.google.co.in/21-01-2015/9:00pm
3. www.scholar.google.co.in/22-01-2015/9:00pm
4. www.cryptographyworld.com/des.htm/27-01- 2015/4:00pm
5. www.google.co.in/22-01-2015/8:15pm
6. www.scholar.google.co.in/22-01-2015/9:00pm
7. www.scholar.google.co.in/23-01-2015/10:00pm
8. www.google.co.in/23-01-2015/10:45pm
9. www.google.co.in/22-01-2015/11:00am