A Comparative Survey Of Symmetric Encryption Techniques For Wireless Devices

Anjali Patil, Rajeshwari Goudar

Abstract: Nowadays, internet and network applications are growing rapidly across the world. Many of the applications, for example e-commerce or e-government, have prime need for security. Information security plays an important role in data communication. Any loss to sensitive data can prove to be great loss to the organization. Encryption algorithm plays main role when confidential data is transmitted over the network. These algorithms consumes a significant amount of computing resources such as memory, battery power, CPU time. This paper provides comparison between different encryption algorithms.

Index Terms: Asymmetric encryption, Key, Security, Symmetric encryption

1 INTRODUCTION

Today, the market for mobile communication and communication devices like cell phones and personal digital assistance(PDA) is growing rapidly. Applications e.g. mobile electronic payment , secure messaging have an inherent need for security. In information security, cryptography algorithms plays an important role. Cryptography converts the original message into the scrambled form. Cryptography ensures that the message should be sent without any modification over the network. The authorized person has the capability to open and read the message.

A. Basic Terms Used in Cryptography

- **Plain Text -**
  The original message is used to communicate with the other is defined as plain text. E.g. Alice send “Hello” message to Bob. Here, “Hello” is a plain text message.

- **Cipher Text -**
  The meaningless message is called as cipher text. In cryptography, the original message is converted into non readable message. E.g. “Pja734” is a cipher text produced.

- **Encryption -**
  Encryption is a process of converting plain text into cipher text. Encryption techniques are used to send secret message through an insecure channel. Encryption process require an encryption algorithm and a key. Encryption takes place at the sender side.

- **Decryption -**
  Decryption is the reverse process of encryption where it converts text into plain text. Decryption takes place at receiver side to obtain the original message from non readable message. Decryption process requires decryption algorithm and a key.

- **Key –**
  A key is a numeric or alpha numeric text. The key is used when encryption takes place on the plain text and at the time of decryption on the cipher text. In cryptography, selection of key is very important since the security of encryption algorithm depends on it.

B. Purpose of Cryptography

Cryptography provides a number of security goals to provide protection to data. Following are the goals of cryptography[1].

- **Confidentiality –**
  Ensures that transmitted information are accessible only for reading by the authorized parties.

- **Authentication –**
  Ensures that origin of message is correctly identified, with an assurance that the identity is not false.

- **Integrity –**
  Ensures that only authorized parties are able to modify the transmitted information. Modification includes writing, changing , deleting of transmitted information.

- **Non repudiation –**
  Requires that neither sender nor the receiver of message should be able to deny the transmission.

- **Access control –**
  Access to information may be controlled by or for the target system.

- **Availability –**
  Requires that information be available to authorized parties when needed.

- *Anjali M. Patil is currently pursuing masters degree program in computer engineering in Maharashtra Academy of Engg , Pune University, India.*
  E-mail: anjalimpatil21@gmail.com
- *Prof.R.M.Goudar M.E Computer Engg., Maharashtra Academy of Engg. Pune University, India.*
- *E-mail: rmgoudar66@gmail.com*

C. Classification of Cryptography

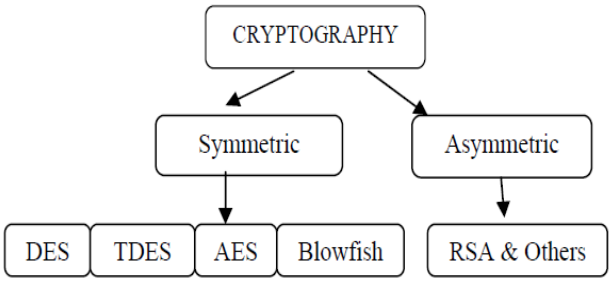

Fig.1. Classification of cryptography

- **Symmetric Encryption –**
  In Symmetric cryptography, same key is used for encryption and decryption. Key plays an important role in cryptography. The key should be distributed before transmission between two parties. The strength of symmetric key encryption depends on the size of the key. Data can be easily decrypted if a weak key is used in the algorithm. There are various symmetric key algorithms such as DES, 3DES , AES ,RSA ,Blowfish[2].

- **Asymmetric Encryption –**
  The problem of key distribution is solved by asymmetric key encryption. In asymmetric key encryption, two different keys are used for encryption and decryption - public and private key. The public key of the receiver is used to encrypt the plain text and only the authorized person can be able to decrypt the cipher text through his own private key. Private key is kept secret.

2 PROBLEM DEFINITION

Various encryption techniques are used in cryptography such as DES,,3DES,AES,RSA etc. The main problem is to select the algorithm with better key length. Other problem is to make choice on the implementation of cryptosystem. The choice of better algorithm depends on the advantages and disadvantages of each algorithm. Symmetric encryption technique have number of benefits. Symmetric encryption uses the same key to encrypt as well as to decrypt. Performance is relatively high. These algorithms can be directly implemented on hardware easily. The weakness of symmetric algorithm is sharing key between two parties. Asymmetric encryption uses two different keys for encryption and decryption. Private key is used to decrypt the encrypted message. Key distribution problem is solved by asymmetric encryption. The public key is known to everyone as it is used for encrypting the message. So, everyone can encrypt the message but, only authorized person can decrypt the message. Performance of asymmetric encryption is relatively low as compared to symmetric encryption. The main problem of asymmetric encryption is it works slower as compared to symmetric encryption.

3 METHODOLOGIES

A. Asymmetric Key Cryptography

RSA:
RSA is most widely used public-key cryptosystem. It provides data confidentiality, key exchange and digital signature. The strength of RSA is factoring large numbers[3]. It is a block cipher. In RSA, the plaintext and cipher text are integers between 0 and n-1 for some n. The description of the RSA algorithm is as follows[4]. Plaintext is encrypted in blocks , with each block having a binary value less than some number n.

Public key components:

n = product of two large primes, p and q

e = a random number relatively prime and less than (p-1)(q-1)

Primary key components:

$D = e^{-1} \bmod ((p-1)(q-1))$, the multiplicative inverse of mod((p-1)(q-1))

Encryption:

$C = M^e \bmod n$

Decryption:

$M = C^d \bmod n$

Digital Signature:

$S = M^d \bmod n$

$M = S^e \bmod n = M^{ed} \bmod n$ (to verify the signature)

The following requirements must be met for RSA to be satisfactory.

1. p and q , two large primes must remain secretive.
2. It is possible to find value of n, e, d such that , $M^{ed} \bmod n$ for all M<n.
3. It is infeasible to determine d , given e and n.
4. It is easy to calculate M^e and C for all values of M<n.

Other Asymmetric Key Algorithm

Other asymmetric key algorithms are used in conjunction with RSA. These other algorithms have their limitations. These algorithms are Diffie–Hellman[5], Digital Signature Algorithm[6], ElGamal[7] and Elliptic Curve Cryptography[8]. The disadvantage of Diffie-Hellman(DH) algorithm is that it is not as versatile as RSA and key generation might be too computationally expensive for the mobile device. Digital Signature Algorithm (DSA) is not as versatile as RSA. Another problem is that the key varies from 512 to 1024 bits , so requiring a strong key size beyond 1024 bits is not possible. DSA is slower than RSA in terms of signature verification[9]. In ElGamal, the cipher text generated is twice the size as the plaintext, therefore it is not suitable in an environment with high latency and low bandwidth. ECC provides equal security for a smaller key size, thereby reducing processing

overhead[10]. So, ECC is more beneficial than RSA.

B. Symmetric Key Cryptography

DES (Data Encryption Standard)
It is a symmetric algorithm, means same key is used for encryption and decryption. DES is a block encryption algorithm. It uses one 64 bit key. Out of 64 bits, 56 bits used as independent key, which determine the exact cryptography transformation and 8 bits are used for error detection. The main operations are permutation and substitution. Bits permutation and substitution are performed in one round of DES. Six different permutation operations are performed both in key expansion and cipher part. Decryption process of DES algorithm is similar to encryption, only the round keys are applied in reverse order. The drawback of this algorithm is, it can be easily prone to Brute force Attack. It is easy for the hacker to break the key by applying all possible combinations. In DES, there are only 2^256 possible combinations which are easy to crack. So DES is not secure[11].

3DES(Triple Data Encryption Standard)
Triple DES is replacement for DES due to advances in key searching[12]. 3DES uses three rounds of DES encryption and has a key length of 168 bits. It uses either two or three 56 bit keys in the sequence Encrypt-Decrypt-Encrypt(EDE). Initially, three different keys are used for the encryption algorithm to generate cipher text on plain text message, t.

$$C(t) = E_{k1}(D_{k2}(E_{k3}(t))) \quad (1)$$

Where, C(t) is cipher text produced from plain text t, E_{k1} is the encryption method using key k1, D_{k2} is the decryption method using key k2 and E_{k3} is the encryption method using key k3. Another option is to use two different keys for the encryption algorithm which reduces the memory requirement of keys in TDES.

$$C(t) = E_{k1}(D_{k2}(E_{k3}(t))) \quad (2)$$

TDES algorithm with three keys requires 2^168 possible combinations and with two keys requires 2^112 combinations. It is practically not possible to try such a huge combinations, so TDES is a strongest encryption algorithm. The disadvantage of this algorithm it is too time consuming[1].

AES(Advanced Encryption Standard)
AES is replacement of DES. AES is a variable bit block cipher and uses variable key length of 128,192 and 256 bits. In AES, there are number of processing rounds. These rounds are based on the key size. If the key length is 128 bits, AES will perform nine processing rounds. If key is of 192 bits, AES perform 12 rounds and if the key size is 256 bits then AES perform 14 processing rounds[13]. Each processing round involves four steps:-

- **Substitute byte :**
  a non-linear substitution step where each byte is replaced with another according to a lookup table.

- **Shift rows :**
  a transposition step where each row of the state is shifted cyclically a certain number of steps.

- **Mixcoloumn :**
  a mixing operation which operates on the columns of the state, combining the four bytes in each column.

- **Add round key :**
  each byte of the state is combined with the round key using bitwise XOR.

AES encryption is fast and flexible. It can be implemented on various platforms especially in small devices.

Blowfish
Blowfish is a 64 bit block cipher and have variable length key from 32 bit to 448bits[14]. This algorithm has two parts – key expansion and data encryption. The key expansion part converts 448bit key into 468bytes A P array of size 18 and four S boxes whose size is 256, each of which are initialized to hexadecimal digits of π. XOR each entry in P array and S boxes with 32 bits of the key[15]. There are 16 rounds of data encryption[16]. In each round a 32 bit subkey is XORed with leftmost 32 bits of plaintext and the result is then passed to the F function of Blowfish. Now, this result becomes rightmost 32 bits for the next round and the output of F function is XORed with the original rightmost 32 bits of plaintext becomes leftmost 32 bits for next round and so on. The f function is distinguishing feature of Blowfish. In Blowfish, key length is 448 bits, s it requires 2^448 combinations to examine all keys[17]. The advantage of this algorithm is, it is simple to implement as all operations are XOR and addition.

Related Work
It is concluded that AES is faster and more efficient than other encryption algorithms [18]. There is insignificant difference in performance of different symmetric key schemes during the transmission of data. It would be better to use AES scheme in case of data transfer.

Comparison
The choice of algorithms depends on user needs and task. DES was designed to work better in hardware than software. DES involves lots of bit manipulation in substitution and permutation. Advanced Encryption Standard (AES) was designed to take into account software and hardware recital, safety measures [19].

TABLE 1
Comparison DES, 3DES, AES

Distinguishing Parameters	DES	3DES	AES
Block Size	64 bit	64 bit	128 bit
Key Size	56 bit	168 bit	128, 192,256 bit
Rounds	16	48	10,12,14
Speed	Low	Moderate	High
Security	Proven Inadequate	Still Insecure	Secure
Resource Consumption	High	Moderate	Low
Algorithm Structure	Fiestel Network	Fiestel Network	Substitution Permutation Network
Attacks	Brute Force Attack	Theoretically possible	Side Channel Attack

4 CONCLUSION

This paper gives a detailed study of the popular symmetric key encryption algorithms such as DES, Triple DES, AES, Blowfish and asymmetric key encryption algorithms such as RSA, D-H etc. The memory requirement of symmetric algorithms is lesser than asymmetric encryption algorithms and symmetric key algorithms runs faster than asymmetric key algorithms. Further, symmetric key encryption provides more security than asymmetric key encryption.

ACKNOWLEDGMENT

My heartfelt thanks to my guide, Prof. R. M. Goudar, Asst Professor, College of Maharashtra Academy of Engineering, Pune, who offered her whole hearted guidance and invaluable suggestions throughout the preparation of this paper. Above all I must and do thank God Almighty from the depth of my heart for the being with me at each and every stage assuring hope, confidence and courage to get the task accomplished in time

REFERENCES

[1] O.P Verma, Ritu Agarwal, Dhiraj Dafouti and Shobha Tyagi, " Peformance Analysis Of Data Encryption Algorithms",IEEE Delhi Technological University , India,2011.

[2] Diaa Salama, Abdul. Elminaam, Hatem Mohamed, Abdul Kader and Mohie Mohamed Hadhoud, "Performance Evaluation of Symmetric Encryption Algorithms", International Journal of Computer Science and Network Security, vol.8 No.12, December 2008.

[3] Brute Schneier 1996. Applied Crypography.2nd ed. New York: John Wileyand Sons. Inc.

[4] William Stallings 2000. Network Security Essentials, application and standards. New Jersey: Prentice Hall.

[5] W.Diffie and M.Hellman November 1976. New Directions in Cryptoraphy. IEEE transactions on Information Theory.

[6] National institute of Standards and technology 1991."Digital Signature Standard – FIPS PUB 186".

[7] T.ElGamal 1985. A Public Key Cryptosystem and a Signature Scheme Based on Diiscrete Logarithms. IEEE transactions on Information Iheory, vol.IT-31,n.4,469- 472.

[8] V.S.Miller 1986. Use of Elliptic Curves in cryptography. Advances in Cryptography- crypto 85 Proceedings, Springer Verlag, 417-426.

[9] Nicolas T. Courtois 2005. Is AES a secure cipher. http://www.nicolascourtois.net.

[10] S.A.Vanstone 2003. Next Generation security for wireless: elliptic curve cryptography. Computer and Security,vol.22.12-144.

[11] Diaa Salama, Abdul Minaam, Hatem M. Abdual-Kader, and Mohiy Mohamed Hadhoud, "Evaluating the Effects of Symmetric Cryptography Algorithms on Power Consumption for Different Data Types", International Journal of Network Security, PP.78-87, Sept. 2010.

[12] Aamer Nadeem and Dr M. Younus Javed , "A Performance Comparison of Data Encryption Algorithms", IEEE, 2005.

[13] Himani Agrawal and Monisha Sharma, "Implementation and analysis of various symmetric cryptosystems", Indian Journal of Science and Technology Vol. 3 No.12, December 2010.

[14] Tingyuan Nie and Teng Zhang," A Study of DES and Blowfish Encryption Algorithm", IEEE, 2009.

[15] Russell K. Meyers and Ahmed H. Desoky, "An Implementation of the Blowfish Cryptosystem", IEEE ,2008.

[16] Allam Mousa, "Data Encryption Performance Based on Blowfish", 47th International Symposium ELMAR- 2005.08-1 0, June 2005.

[17] Michael C.-J. Lin and Youn-Long Lin, "A VLSI Implementation of the Blowfish Encryption/Decryption Algorithm", IEEE, 2000.

[18] Nagesh Kumar, Jawahar Thakur, Arvind Kalia on "PERFORMANCE ANALYSIS OF SYMMETRIC KEY CRYPTOGRAPHY ALGORITHMS:DES , AES and BLOWFISH " in An International Journal of Engineering Sciences ISSN: 2229-6913 Issue Sept 2011, Vol. 4 ,pp.28-37.

[19] Hamdan.O.Alanazi, B.B.Zaidan, A.A.Zaidan, Hamid A.Jalab, M.Shabbir and Y. Al-Nabhani, "New Comparative Study between DES, 3DES and AES "[ISSN 2151-9617].