Enhancement of Local Languages in DES

V.Sivakumar (*Ph.D scholar*)
Dept of CSE, VIT CHENNAI CAMPUS
Chennai, India
sivakumar.v2013@vit.ac.in

Mithra.S (*Asst. Professor*)
Dept of CSE, Easwari Engineering College
Chennai, India
mithrasamuel@gmail.com

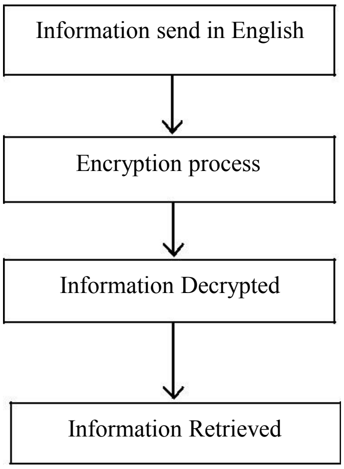
***Abstract*— Network services and internet plays vital role in transmitting information from source to destination. The transmitted information undergoes security attacks by the hackers. Hacker uses several attacks to retrieve the information. Most widely used algorithm to secure the information is the DES algorithm. The only limitation with this algorithm is to withstand the brute force attack which is due to the less number of possible keys. To overcome this limitation the DES algorithm is enhanced. In this paper we propose to implement private key which is used in non-English (local language). The advantage of this enhancement is, the attacker cannot predict the local language and hence the brute force attack becomes much difficult thus enhancing the security of the system.**

***Keywords*— brute force attack; transliteration; unicode; symmetric encryption; block ciphering**

I. Introduction

Cryptography is a technique which is used to secure transmitting information. The process includes encryption and decryption. Secret key is used in the process to convert the plaintext into encrypted format. Symmetric key and asymmetric key cryptography are the two classification of cryptography .DES is the one the symmetric key cryptography where the same key is used in the encryption and decryption process. Fig. 1 illustrates the standard encryption and decryption process.

Fig. 1 Encryption and decryption process



Ojha et al. (2012) developed a software tool involves cryptographic enciphering and deciphering along with File Splitting and Merging mechanisms. In this approach a file which has secret data is sliced into desired number of pieces upon user's specification and then the cryptographic encryption phase is carried out. In this paper, differentiate the cryptographic scheme by providing different key for each encryption of sliced files; provided the key should be given correctly at the time of decryption to avoid erroneous results.

Charles Cornell proposed a new method to enhance the performance of the Data Encryption Standard (DES) algorithm has been proposed by replacing the predefined XOR operation applied during the 16 round of the standard algorithm by a new operation depends on using two keys, each key consists of a combination of 4 states (0, 1, 2, 3) instead of the ordinary 2 state key (0,1).

Shah Kruti (2012) proposed a method where in message is encrypted by representing it as a number M, raising M to a publicly specified power e, and then taking the remainder when the result is divided by the publicly specified product, n, of two large secret prime numbers p and q. The security of the system rests in part on the difficulty of factoring the published divisor, n.

Shasi et al. (2011) developed system uses 84-bit initial key instead of the 56-bit key originally used. It has substitution boxes inside the key generation algorithm and mod2 additions. The choice of arrangement of substitution boxes in the main algorithm for each round is sub substitution boxes in the main algorithm for each round is sub-key dependent.

Wuling Ren (2010) proposed to enhance the security of data transmission in Bluetooth communication, a hybrid encryption algorithm based on DES and RSA is proposed. The currently used encryption algorithm employed by the bluetooth to protect the confidentiality of data during transport between two or more devices is a 128-bit symmetric stream cipher called E0.

ASCII and EBCDIC code was developed by using only English character and word. It was very difficult to represent the language with huge number of characters. UNICODE uses 16 bit decimal code. For example, Tamil has 128 code values from 0B80-0BFF.

IJERT

II. Data encryption standard

DES is a previously predominant symmetric- key algorithm for the encryption of electronic data. Large amount of information is transmitted in a network service. It was highly influential in the advancement of modern cryptography in the academic world. While transferring information the DES technique partition them as block and encryption is performed in block by block manner. DES is widely used in many applications while brute force is the limitation. DES includes the following:

A. Intial permutation

The process includes reordering of the 64 bits from the given input.

B. Rounds:

The process includes 16 rounds. All the 16 rounds perform the same operation. The operation includes the 64 bit get partitioned into two 32 bits one in the left side and the other in the right side (Li-1, Ri-1). The 32 bit in the right side get shifted into left side to generate Li. The 32 bit in the right side undergo expansion/permutation stage and become 48 bits and it involves Ex-or operation along with its key. The Ex-ored 48 bit undergo S-BOX to reduce itself to 32 bit and get permutated. The permuted 32 bit of the Ri-1 is Ex-ored with 32 bits of the Li-1 to generate Ri.

C. Inverse initial permutation:

It reorders the bits present in the previous stage.

D. Key Generation:

Key generation process involves permuted choice and left circular shift. Among the 64 bit key last 8 bits are discarded and the 56 bit enter into the left circular shift from the permuted choice1. After the permuted choice 2 the output will be 48 bit.

IJERT

III. UNICODE

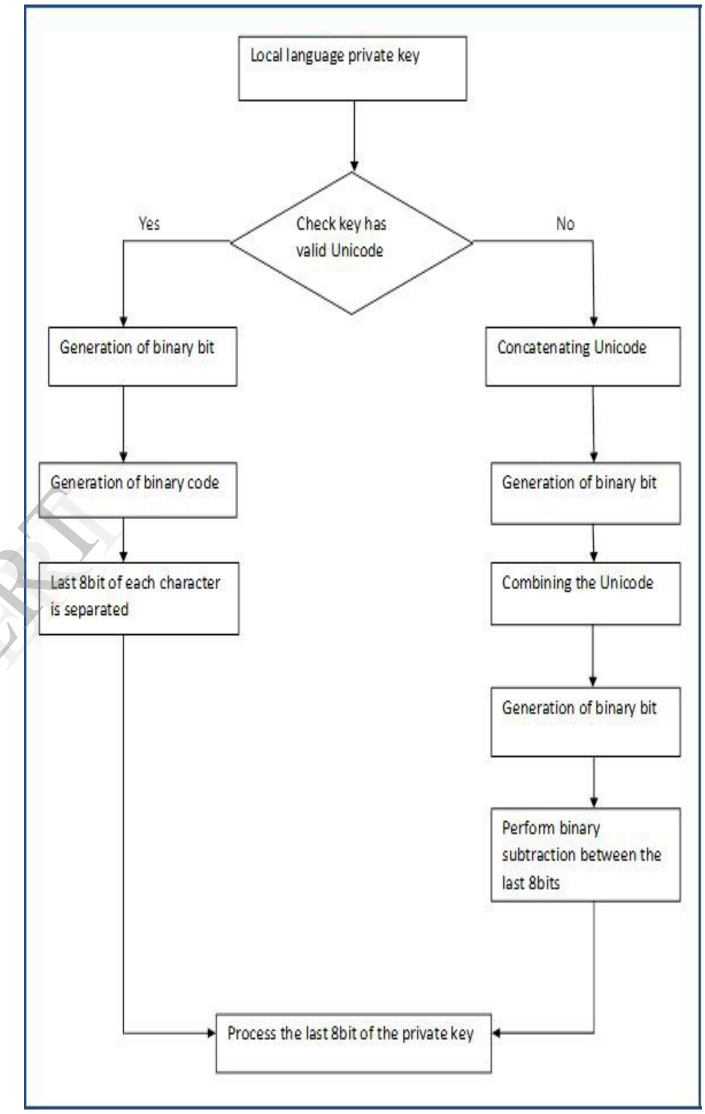
ASCII can support only the countable number of characters. So, it is a common thing in everybody's mind the encryption process involves normalization, decomposition, collation etc. by using these countable number of characters. Unicode concept is introduced so as to handle the Multilanguage text to achieve internationalization. It overcomes limitation while using ASCII code. It can support more than 100 languages. It enable the user to use more number of keys than ASCII permits.

IV. PROPOSED SYSTEM

In these enhanced DES algorithm using local language, the private key is given in non-English (Tamil) language to perform both encryption and decryption process. The Non-English key is implemented by the process of transliteration in which the language is converted from one format of text into other format of text by the use of Unicode.

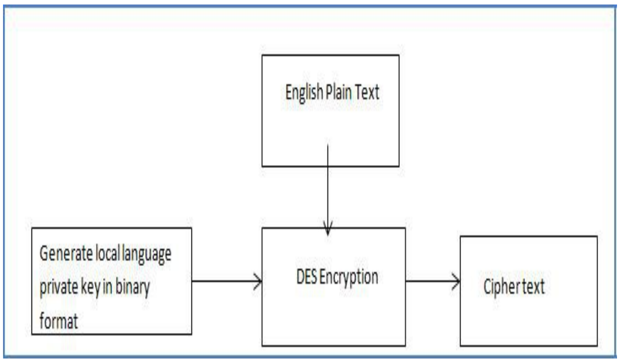
Transliteration is a process which is used to represent the one language text into another form of language text .In these criteria transliteration operation is used to give the private key in local languages. This is achieved by Unicode But some of the characters cannot be represented using single Unicode. At this situation combination of Unicode is used to represent the single letter. While forming the key, the last 8 binary bit is used as key instead of each character to reduce the computation time to perform the operation and also it will avoid guessing of password due to the usage of repeating character of most significant bits. Fig. 2 illustrates the mechanism for generation of non-English private key.

Fig.2 Generation of non-English private key


Local language private key
Yes
Check key has valid Unicode
No
Generation of binary bit
Concatenating Unicode
Generation of binary code
Generation of binary bit
Last 8bit of each character is separated
Combining the Unicode
Generation of binary bit
Perform binary subtraction between the last 8bits
Process the last 8bit of the private key

In the situation of using multiple Unicode to represent the single character where the letter of the private key is formed by performing binary subtraction between the last 8bit of those characters. Then these Binary bits are used as the input key of the both encryption and decryption process of DES technique as shown in Fig. 3 and 4 respectively.

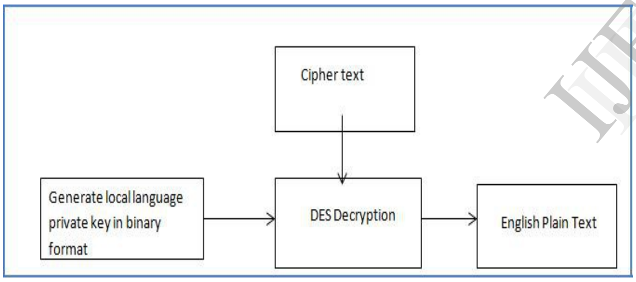
Fig. 3: Enhancing DES encryption process using local language key



English is the most widely used language by the many people hence these technique uses key alone in local language to perform the encryption to increase the possible number of keys by using the local language. The local language key and English plain text which is used as the DES encryption process to generate cipher text.

Ciphertext which is generated by encryption process and formed binary bit of local language key as input to the DES decryption process to retrive the original information.

Fig. 4: Enhancing DES decryption using local language keys



V. Test Results

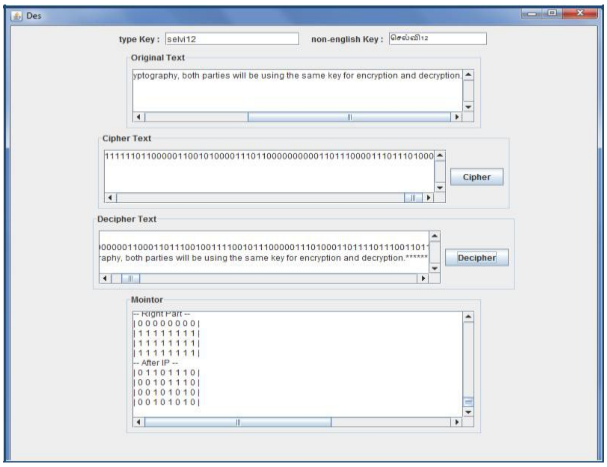
Let us consider the case in which tamil is the local language key:

Every character has the Unicode value which is mapped into English letters to perform transliteration. That is, while typing the input in English language it will automatically converted into corresponding Tamil letters. For example, a/A is mapped into Tamil letter அ Unicode value “U085”. The utf-8 binary representation of corresponding this letter is 11100000 10101110 10000101. Hence last 8bit 10000101 is taken as input for the corresponding letter அ. Some characters which is not supported by single Unicode is representation will be processed as shown below.

The character க் is represented by combination of க and ் Symbols of Unicode value “U0B82 U0B95”. Then binary subtraction of last 8 utf-8 binary character and output will be given as key for the corresponding character.

In this implementation, the plaintext is first given and then followed by the secret key in local language to perform the encryption process. This enciphered text will be given to the input for the decipher text. Then, decryption is performed to generate the original text. In monitor all process which has taken place will be monitored at each and every step as shown in Fig. 5.

Fig. 5 Screenshot of enhanced DES implementation.



type Key : selvi12

non-english Key : செல்வி12

Original Text

yptography, both parties will be using the same key for encryption and decryption.

Cipher Text

```
11111101100000110010100001110110000000000110111000011101110100
```

Decipher Text

```
)000001100011011100100111100101110000011101000110111101110011011
aphy, both parties will be using the same key for encryption and decryption.******
```

Mointor

```
-- Right Part --
|00000000|
|11111111|
|11111111|
|11111111|
-- After IP --
|01101110|
|00101110|
|00101010|
|00101010|
```

VI. Conclusion

The limitation of DES technique due to the brute force attack can be rectified on enhancing the DES using local language by introducing the private key in the local language and increasing the possible number of keys more than the ASCII. The last 8 bit is used to reduce the computation power of system and avoid the prediction of cipher text using the repeated most significant binary bits. Overall performance of the cryptography increases due to performance increase in most widely used DES technique in many applications by using non-English language keys.

References

[1] Atul Kahte, "Cryptography and Network Security",Tata Mcgraw Hill, 2007.

[2] Charels Connell, "An Analysis of New DES: A Modified Version of DES", Locust Street Burlington, USA Boston MA 02215 USA.

[3] D.B. Ojha, Ramveer Singh, Ajay Sharma, Awakash Mishra and Swati garg, "An Innovative Approach to Enhance the Security of Data Encryption Scheme. International Journal of Computer Theory and Engineering",Vol.2,No.3, 2010.

[4] Diaasalama, Abdul kader, MohiyHadhoud, "Studying the Effect of Most Common Encryption Algorithms"International Arab Journal of e-technology, vol 2,no.1,January 2011.

[5] Manikandan. G, Rajendiran.P, Chakarapani.K, Krishnan.G, Sundarganesh.G,"A Modified Crypto Scheme for Enhancing Data Security", Journal of Theoretical and Advanced Information Technology, 603-607, 2012.

IJERT

[6] Shah Kruti R., Bhavika Gambhava,"New Approach of Data Encryption Standard Algorithm", International Journal of Soft Computing and Engineering (IJSCE), ISSN: 2231-2307, Volume-2, Issue-1, March 2012.

[7] Shasi Mehlrotra seth, Rajan Mishra,"Comparative Analysis of Encryption Algorithms For Data Communication"IJCST Vol. 2, Issue 2, June 2011.

[8] William Stallings, " Cryptography and Network Security Principles and Practices", Prentice Hall, November 16,2005

[9] Wuling Ren, "A Hybrid Encryption Algorithm Based on DES and RSA in Bluetooth Communication", Second International Conference on Modeling", Simulation and Visualization Methods (WMSVM), 2010.

[10] www.unicode.orgs

IJERT