A NOVEL APPROACH FOR PROVIDING SECURITY TO MESSAGES WITH DYNAMIC-KEY ALGORITHM

DODDA NARASIMHA RAJU, PATTEM SUNIL

Abstract : The modern era is dominated by paperless offices, E-mail messages, E-Cash Transactions, Virtual departmental stores etc. But for the few decades of their existence, computer networks were primarily used by university researchers for sending e-mail and by corporate employees for sharing printers. Under these conditions, security did not get a lot of attention. With the growth of networked multiple media systems, the need of secured data transfer increases. For example data being transferred via networks e.g. the internet, mobile telephones, wireless microphones, bluetooth devices, an automatic teller machines, etc. A cipher is a character-for-character or bit-for-bit transformation, without regard to the linguistic structure of the message. The messages to be encrypted, known as the plaintext, are transformed by a function that is parameterized by a key. The output of the encryption process, known as the cipher text, is then transmitted, often by messenger or radio. Two forms of encryption techniques: Substitution and Transposition. This paper focused on well known transposition cipher, aim is to induce some strength to these ciphers by generating automatic key based on the given message using dynamic- key generation method. This proposed method ensures that it is better in terms of providing more convenient to produce key automatically and more security to any given message.

Keywords: dynamic-key, cipher text, transposition, cryptography, encryption, substitution

Introduction : Cryptography comes from the Greek words for "secret writing." It has a long and colorful history going back thousands of years. Professionals make a distinction between ciphers and codes. A cipher is a character-for-character or bit-for-bit transformation, without regard to the linguistic structure of the message. In contrast, a code replaces one word with another word or symbol. Codes are not used any more, although they have a glorious history.

Cryptography is an art and science of converting plaintext to a cipher text form. To secure the information over communication channels different techniques such as cryptography, stenography, watermarking etc are being implemented. While protecting the confidential information, cryptography provides high level of security. Cryptography involves three different techniques viz. encryption / decryption, linguistic and mathematical formulation for securing information, particularly during communication. Cryptography focuses on keeping the contents of information secret. In general cryptography was concerned solely with encryption. Encryption is the means of converting information form its normal, comprehensible form into an incomprehensible format, rendering it unreadable without secret knowledge. Decryption is reverse of encryption [3].

Two Fundamental Cryptographic Principles:

Cryptographic principle 1: Redundancy - Messages must contain some redundancy

The first principle is that all encrypted messages must contain some redundancy, that is, information not needed to understand the message.

Cryptographic principle 2: Freshness - Some method is needed to foil replay attacks

One such measure is including in every message

a timestamp valid only for, say, 10 seconds. The receiver can then just keep messages around for 10 seconds, to compare newly arrived messages to previous ones to filter out duplicates. Messages older than 10 seconds can be thrown out, since any replays sent more than 10 seconds later will be rejected as too old.

ENCRYPTION TECHNIQUES

Encryption was used primarily to ensure secrecy in important communication systems, such as spies, military leaders and diplomats. Encryption can be used to protect data "at rest", such as to secure it as it is often difficult to physically secure all access to networks. It is also used to protect data in transit, for example data being transferred via networks e.g. the internet, e-commerce), mobile telephones, wireless microphones, wireless intercom systems, Bluetooth devices and an automatic teller machines. There have been numerous reports of data in transit being intercepted in recent years. [7] Encrypting data in transit also helps techniques of encryption. Two building blocks of encryption are Substitution and Transposition[4].

Substitution Ciphers: In a substitution cipher each letter or group of letters is replaced by another letter or group of letters to disguise it. One of the oldest known ciphers is the Caesar cipher, attributed to Julius Caesar. In this method, a becomes D, b becomes E, c becomes F, ..., and z becomes C. For example, attack becomes DWWDFN.

The next improvement is to have each of the symbols in the plaintext, say, the 26 letters for simplicity, map onto some other letter. For example,

plaintext: a b c d e f g h i j k l m n o p q r s t u v w x y z

ciphertext: Q W E R T Y U I O P A S D F G H J K L Z X C V B N M

Transposition Ciphers

Substitution ciphers preserve the order of the plaintext symbols but disguise them. Transposition ciphers, in contrast, reorder the letters but do not disguise them depicts a common transposition cipher, the columnar transposition.

For example, the key given to encrypt and decrypt is IEFLUABTS and plaintext is as follows:

Life is Beautiful.

Then the transposition method is applied as follows:

I E F L U A B T S

5 3 4 6 9 1 2 8 7

PLAIN TEXT: Life is Beautiful.. (length = 18)

l i f e i s b e a

u t i f u l

CIPHER TEXT: slbitfiluefaeiu (length = 15)

The cipher is keyed by a word or phrase not containing any repeated letters. In this example, IEFLUABTS is the key. The purpose of the key is to number the columns, column 1 being under the key letter closest to the start of the alphabet, and so on. The plaintext is written horizontally, in rows, padded to fill the matrix if need be. The ciphertext is read out by columns, starting with the column whose key letter is the lowest.

It offers complete security, but in practice, has two fundamental difficulties:

For every message to be sent, a key of some length is needed by both sender and receiver. Making of large quantities of random keys or defining a key directly for both encryption and decryption is more difficult, in practical. Thus a mammoth key distribution problem exists. Even more overwhelming is the problem of key distribution and protection..

Because of these difficulties, the one-time generation key is of limited utility, and is useful purely for low-band width channel requires very high security. In this nowhere considering the full text including spaces and special characters like . , ; etc.

The keyword may contains repetitive characters, that adds columns to the grid.

Proposed Method

To encrypt a message, key is needed that is same as text contains alphabet letters. here the key generates, not contains repetitive words. Therefore it makes shorten the keyword. The steps required to generate a dynamic key is as follows:

Plaintext : P – an original message

Ciphertext : C – an encrypted message

Key: K – keyword that is generated from computation

Input: Message (P) – An original message

Step 1: assign N = len(P) // including space and other special characters

Step 2: to define a key:

i. find the frequency count of each character in P, excluding special characters
ii. arrange them in descending order based on their frequency count
iii. convert it into a string and add to K

Step 3: Using the keyword K, ordering the columns by the lexicographic order of the letters in the key word.

Step 4: Write the plaintext(P) out in a grid where number of columns is the number of letters in the keyword.

Step 5: steps to obtain ciphertext

i. Take the letter in the key in alphabetical order
ii. Read down the column character by character including special character and add it to C
iii. Continue this process until all columns has read

Step 6: Convert C into a String

Step 7: Stop

The above algorithm illustrates that the process begins by scanning the message P and assign it's length to N, obtain the frequencies of each individual character identified, make arrange them in sorted (descending) order according to their frequency count and it's alphabetic order if the frequency count of two or three letters is same. Later convert them into a string and add to K, treat it as a keyword. Write the keywords above the grid of the plaintext, and also the numbers telling us which order to read the columns in. starting with the column headed by first letter in alphabet order, ciphertext begins reading character by character in this column. Now move to the column headed by second letter in key as in alphabetic order, and so on through the letters of the keyword in alphabetical order to get the ciphertext. As a result, final cipher text is obtained in C.

Experiment

For example, if the message "Life is Beautiful." is encrypted as follows:

Plaintext (P): Life is Beautiful.

In the above message the number of individual characters as follows:

individual alphabet characters - 9

space characters - 2

dot characters - 1

Now consider only the alphabets to form a key. They are a, b, e, f, i, j, s, t, u and frequency counts of each individual letter as follows:

i-3, e-2, f-2, l-2, u-2, a-1, b-1, t-1, s-1

Convert them into as string and add to K, treat it as a key. The key is as follows :

Key (K) : iefluabts (length = 9)

Therefore we can write K as follows

I	E	F	L	U	A	B
	T	S				
5	3	4	6	9	1	2
	8	7				
L	i	f	e		i	s
		B				
E	a	u	t	i	f	u
	l	.				

PLAIN TEXT: Life is Beautiful.. (length = 18)

CIPHER TEXT: ifsiafuleetb. l i (length = 18)

Therefore ciphertext (C) is as follows :

ifsiafuleetb. l i (length = 18, including space & special characters)

Decryption is very simple, obtain the original text just by reverse the above process. As an example, we shall decrypt the ciphertext "ifsiafuleetb. l I" given the keyword "iefluabts". we start by writing out the keyword and the

order of the letters. There are 18 letters in the ciphertext, and the keyword has 9 letters, so we need 18 / 9 = 2 rows.

Now we start by filling in the columns in the order of the keyword, starting the first column is entered towards right. We continue to add columns in the order specified by the keyword. Now we read off the plaintext row at a time to get “Life is Beautiful.”.

Conclusion : The proposed method cipher is simple type of cipher and provides more secure to the messages by generating a secret key automatically based on the given message. This would reduce more time when we need to generate a key. The final cipher text is in strong that is very difficult to break. This method uses transposition method that only reorder the letters in a specific way. There is nothing to worry about the generation of key and its length. The above described method is flexible and useful when the given text length is long and should contain repetitive characters. Therefore this method ensures much more secure and strong cipher.

References

1. William Stalling ”Network Security Essentials”, Pearson Education,2004
2. Atul Kahate (2009), Cryptography and Network Security, 2nd edition, McGraw-Hill.
3. Stallings W (1999), Cryptography and Network Security, 2nd edition, Prentice Hall.
4. William Stallings (‘03), Cryptography and N/w Security, 3rd edition, Pearson Education
5. V. Umakanta Sastry1, N. Ravi Shankar2, and S. Durga Bhavan “A Modified Hill Cipher Involving Interweaving and Iteration” International Journal of Network Security, Vol.11, No.1, PP.11{16, July 2010
6. M. S. Hwang and C. Y. Liu, \ Authenticated encryption schemes: current status and key issues," International Journal of network security, vol.1, no.2, pp.61-73, 2005
7. M.H.Ibrahim, \A method for obtaining deniable public-key encryption, "International journal of n/w security, volume.8,no.1, pp.1-9,09
8. M.H.Ibrahim, \Receiver-deniable public - key encryption," International Journal of network Security, volume.8, no. 2, pp. 159-165, 2009
9. Results of Comparing Tens of Encryption Algorithms Using Di®erent Settings-Crypto++ Benchmark, Retrieved Oct. 1, 2008. (http://www.eskimo.com/ weDai/benchmarks.html)
10. Y. C. Hu, A. Perrig, and D. B. Johnson, “SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks” Proceeding of IEEE Workshop on Mobile Computing Systems and Applications, 2003.
11. International Journal of Advanced Research in Computer Science & S/w engineering. Vol.2, Issue 10, Oct’12 ISSN: 2277 128X “Enhancing Security of Caesar Cipher by Double Columnar Transposition Method” Mr. Vinod Saroha ,Suman Mor, D. Anurag.
12. “Enhancing security of Caesar cipher using different methods”, Anupama Mishra, International Journal of Research in engineering & Technology eISSN:2319–1163|pISSN:2321– 7308.
13. Foundations of Cryptography: Volume 2, Basic Applications. Cambridge university press, 2004.

Assistant Professor, Department of Computer Science, Shri Vishnu Eng. College for Women, Bhimavaram, W.G.District, Andhra Pradesh, India. E-mail : dnraju@svecw.edu.in, Phone No: +91-9949072448

Pattem Sunil, Assistant Professor, Department of Computer Science, Shri Vishnu Eng. College for Women, Bhimavaram, W.G.District, Andhra Pradesh, India. E-mail : sunilp@svecw.edu.in, Phone No: +91-9493237923