Volume No:4, Issue No:3 (August-2018) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Review on Layered Cryptography

D.Sreenu Babu
Department of Computer Science & Engineering, Aditya Institute of Technology and Management, Tekkali, K Kotturu, Andhra Pradesh 532201, India.

B.Ramesh
Department of Computer Science & Engineering, Aditya Institute of Technology and Management, Tekkali, K Kotturu, Andhra Pradesh 532201, India.

Introduction to Cryptography:

Security and privacy are critical for electronic communication and e-business. Network security measures are needed to protect data during its transmission. Cryptography plays a vital role in network security as it allows two parties to exchange sensitive information in a secured manner. The word cryptography means covered writing(covered for crypto and writing for graphy) [1]. It involves the use of a secret key known only to the participants of the secure communication: If A wants to send a message to B, he encrypts the original message X by the encryption algorithm using the key agreed upon by them. The encrypted message is transmitted through the communication media and the key is transmitted through a secured media like RF cable, fibre, etc. The receiver decrypts the original message from the encrypted message using the same key and the decryptor. A cryptanalyst may try to capture the message and the key. If he fails to do so, the encryption algorithm is successful [2].

CRYPTOGRAPHY:

When it comes to the security of any important data, the first solution what strikes is encoding the actual data in some form which is private to the user/users only[3]. In technical terms, the simplest solution is Cryptography.

What is cryptography?

Cryptography is the art of achieving security by encoding messages to make them non-understandable to others. Forming an intelligible message into unintelligible one and then re-transforming that message back to its original form is Cryptography.

There are two types of cryptography:

- Asymmetric Cryptography
- Symmetric Cryptography

If the sender and the receiver use different keys, its called asymmetric or multiple-key, public-key encryption. If the sender and the receiver use the same key, it is called symmetric or single-key, secret-key or conventional encryption.

Encryption: It is the technique of converting original text into coded text using particular key.

Decryption: It is the technique of converting coded text into original text using some key. Whereas the original text known as plain text and coded text is known as cipher text.

What is Imbricate cryptography?

Imbricate cryptography is a new technique that uses the layered approach designed by us. It is a type of symmetric cryptography in which the key is implanted in the message, so the message cannot be recovered without using the correct key. Here the message and the key are inwardly plaited [4]. It involves layers of encryption and decryption. Since the key is of variable length of the users choice, it cannot be found by permutation and combination. Moreover, the output transmitted as a bitmap file perplexes the cracker. Thus the encrypted file can be sent across the network of interest.

Cite this article as: D.Sreenu Babu & B.Ramesh, "Review on Layered Cryptography", International Journal of Research in Advanced Computer Science Engineering, Volume 4, Issue 3, 2018, Page 9-13.

Volume No:4, Issue No:3 (August-2018) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Implementation is done by us for the message involving text but the algorithm is extensible to any media. Simplicity, user-orientation and compatibility are the key features of the algorithm.

Notion of encryption:

The algorithm extends to three layers of encryption, each having its own importance.

Layer-1-

It is called the mapping layer and juggles the cracker by jumbling characters. Here each of the characters is replaced with another one present in the same set. There are two types of sets: repeated characters and non-repeated characters. English words consist of alphabets, in which the probability of occurrence of some characters such as ,a, ,e, ,i, ,o and ,r is maximum [5]. These characters are called repeated characters. Others are non-repeated characters, i.e., they are repeated occasionally. Each and every character of the source file is mapped with a character present in the same set, thus providing the first layer of cryption. This layer does not include the password or key. Equivalent mapping characters for source file characters are shown in the table. The numbers are also replaced, causing mismatch in numbering also.

Layer-2-

It is called the core-encoding layer as it exploits the bitwise logics and ASCII format to encode each character. Here each character formed by layer-1 is transmuted to an ASCII character, which is not a usual symbol (alphabet, special character or number). The first character of the message obtained by layer-1 is XORed with negated ASCII character of the first character of the password [6]. This process is carried out for the rest of the message. Since the password is of a small length, it is repeatedly applied to the message.

This can be formulated as follows:

Char_new = (Char_old) ^ (~key[i])

Layer-3-

It is called the bitmap-conversion layer as it converts ASCII characters into the equivalent binary value and stores the result as a bitmap file [7]. This is done by just obtaining the binary equivalent of the resultant ASCII characters of layer-2 and writing it into a file that is bitmap in nature.

An example for a specific case-

Let us illustrate our technique by the following sets:

Message M ={hello• };

Key K ={hai• };

Layer-1:

Table for Mapping

Source file characters	Equivalent mapping characters
a/e/i/o/s/t/ {repeated}	o/t/s/i/a/e/
b/c/d/e/f/g/h/j/k/l/m/n/ p/q/r/u/v/w/x/y/z/ {non-repeated}	h/f/b/d/g/c/l/n/j/k/m/u/y/p/z/q/v/w/x/p/
0/1/2/3/4/5/6/7/8/9/ {numerals}	4/6/9/7/0/8/1/3/2/5/
Special characters	Same characters

From the table, we can replace

M1={ltjji• };

Layer-2:

M2 = M1 ^(~K);

M2 ={l^~h, t^~a, j^~i, j^~h, i^~a};

M2 ={1032~• };

Note that XOR operation is represented by symbol ,^, 1s complement operation is represented by symbol ,~, and binary values are 11111011, 11101010, 11111100, 11111101 and 11101111. These binary numbers are put in the character form in the output bitmap file finally. An important criterion entailed here is that there is no one-to-one mapping of message characters and password characters [8]. This can be well understood by looking into the above example. Observe that for the same character j, the resultant codes are not the same. That is, the first ,j is replaced with 11111100 and the second, j is replaced with, 11111101. This shows that the resultant code is unpredictable even for the same set of characters.

Volume No:4, Issue No:3 (August-2018) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Algorithm for encryption-

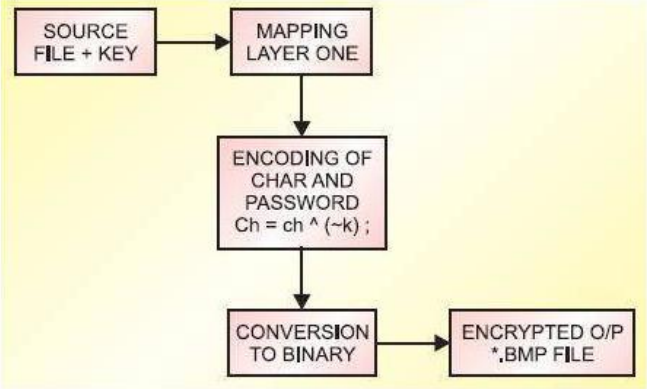
1. Get the source file and the password (key) from the user.
2. Choose a mapping character for each character present in the file using the table.
3. Replace the original character with the mapping character. This is the end of layer-1.
4. Using the password (key) received from the user, encode each character of the message with the successive character of the key.
5. The formula for encoding is:
char_new = (char_old) XOR (~key[i]).
This is the end of layer-2.
6. The resultant character is converted into the binary form. This is the end of layer-3.
7. Write the binary values of the new characters in the output bitmap file.
From the table, we can replace
M1={ltjji• };

Layer-2:

M2 = M1 ^(~K);
M2 ={l^~h, t^~a, j^~i, j^~h, i^~a};
M2 ={1032~• };
Note that XOR operation is represented by symbol ,^, 1s complement operation is represented by symbol ,~, and binary values are 11111011, 11101010, 11111100, 11111101 and 11101111. These binary numbers are put in the character form in the output bitmap file finally. An important criterion entailed here is that there is no one-to-one mapping of message characters and password characters [9]. This can be well understood by looking into the above example. Observe that for the same character j, the resultant codes are not the same. That is, the first ,j is replaced with 11111100 and the second, j is replaced with, 11111101. This shows that the resultant code is unpredictable even for the same set of characters.

Algorithm for encryption-

1. Get the source file and the password (key) from the user.
2. Choose a mapping character for each character present in the file using the table.
3. Replace the original character with the mapping character. This is the end of layer-1.
4. Using the password (key) received from the user, encode each character of the message with the successive character of the key.
5. The formula for encoding is:
char_new = (char_old) XOR (~key[i]).
This is the end of layer-2.
6. The resultant character is converted into the binary form. This is the end of layer-3.
7. Write the binary values of the new characters in the output bitmap file.



Notion of decryption-

Decryption is done in the reverse order of encryption. It also has three layers like encryption. Let us go through each layer of the algorithm.

Layer-1-

It is called character-restructuring layer and regroups the bits from the bitmap file to form characters (ASCII). For each 8-bit data found in the original bitmap file, we find the equivalent ASCII value. Then the character formed by that ASCII is found and noted.

Layer-2-

It is called the core-decoding layer. One of the most fascinating things in XOR logic is that if we apply it twice, the original character can be reproduced. This reveals that the algorithm used in encryption (layer-2) can also be utilized for decryption also.

Volume No:4, Issue No:3 (August-2018) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

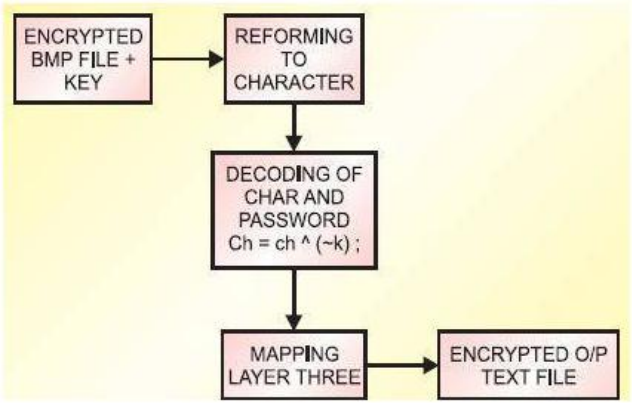
Thus the same bitwise logic is used here too. Note that only the same key as used in encryption can retrieve the message back.

Layer-3-

It is called the re-mapping layer and works like layer-1 of encryption in the reverse direction. It finds the character in column II of the table and replaces it with the equivalent character present in column I of the table. This completes the decryption process and the output character is written back to the file for decryption. Note that both the encryption and the decryption processes consist of one layer (layer-1) independent of the key and the other layers are dependent on the key. Thus now we can know why layer-1 of encryption has not included key.

Algorithm for decryption-

1. Get the bitmap file and the key from the user.
2. Read the binary values from the file and convert back into characters. This is the end of layer-1.
3. From the password (key) received from the user, decode each character with successive character of the key.
4. The formula for encoding is:
char_new = (char_old) XOR (~key[i]);
This is the end of layer-2.
5. Choose a mapping character for each character using the table in the reverse order.
6. Replace the original character with the mapping character. This is the end of layer-3.
7. Write the decrypted character in the output file.



System performance:

Any person who wants to crack this system must:
1. Know that the binary values in the bitmap represent ASCII value of the encrypted character.
2. Read the binary values from the bitmap file and convert them into characters.
3. To break the second layer, find the logic that the key is XORed with the characters. (The key should be known.) But finding the key, which is transmitted over a secured channel, is not possible.
4. Then find the mapping characters to break the first layer. Use of the permutation and combination method for finding the key is impossible. Hence the system performance is good.

Advantages of the system:

1. Confidentiality.
No user can access the message without using the correct key.
2. Simplicity.
The system can be implemented (only for text messaging) through a very simple ,C program given at the end of this article.
3. Security.
The system is secure because the key is sent through a secret medium and the message cannot be recovered without the key.
4. Protection.
It is provided by the key as it controls the access to the message.
5. Incorporated key.

Many cryptography techniques use the key for only access control. Our system integrates the key with the message, so the message can be separated from the key only if the correct key is produced. Imbricate cryptography involves layers of encryption and decryption. Since the key is of variable length of the user's choice, it cannot be found by permutation and combination. Moreover, the output transmitted as a bitmap file perplexes the cracker.

Volume No:4, Issue No:3 (August-2018) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Thus the encrypted file can be sent across the network of interest.

Applications:

Identification and Authentication:

Identification and authentication are two widely used applications of imbricate cryptography. Identification is the process of verifying someone's or something's identity. Authentication merely determines whether that person or entity is authorized for whatever is in question. For this purpose Digital signatures are used.

Certification:

It's a scheme by which trusted agents such as certifying authorities vouch for unknown agents, such as users. The trusted agents issue vouchers called certificates which each have some inherent meaning. Certification technology was developed to make identification and authentication possible on a large scale.

Personal Use:

Privacy is perhaps the most obvious application of imbricate cryptography. Privacy is the state or quality of being secluded from the view and or presence of others. Imbricate cryptography can be used to implement privacy simply by encrypting the information intended to remain private. In order for someone to read this private data, one must first decrypt it. Note that sometimes information is not supposed to be accessed by anyone, and in these cases, the information may be stored in such a way that reversing the process is virtually impossible.

Passwords:

Passwords are not typically kept on a host or server in plaintext, but are generally encrypted using some sort of hash scheme. In the Windows NT case, all passwords are hashed using the MD4 algorithm, resulting in a 128-bit (16-byte) hash value.

References:

[1] E. J. Byres SCADA Security 2012 Crystal Ball Tofino Security 2012 [online] Available: http://www.tofinosecurity.com/blog/scada-security-2012-crystal-ball.

[2] G-. W. Arnold "Challenges and Opportunities in Smart Grid: A Position Article" Proc. IEEE. vol. 99 no. 6 pp. 922-27 2011.

[3]L. Lamport "Password Authentication with Inesecure Communication" Commun. ACM vol. 24 no. 11 pp. 770-72 1981.

[4] Information Assurance Technical Framework (IATF) Release 3.0 National Security Agency 2000 [online] Available: http://www.dtic.mil/dtic/tr/fulltext/u2/a393328.pdf.

[5] Cryptlib Encryption Toolkit [online] Available: http://www.cs.auckland.ac.nz/-pgut001/cryptlib/.

[6] X-. Wang H. Yu "How to Break MD5 and Other Hash Functions" Proc. 24th Annual Int'l. Conf. Theory and Applications of Cryptographic Techniques pp. 19-35 2005.

[7] M. Majdalawieh F. Parisi-Presicce D. Wijesekera "DNPSec: Distributed Network Protocol Version 3 (DNP3) Security Framework Advances in Computer Information and Systems Sciences and Engineering" pp. 227-34 2006.

[8] I. Noi Fovino "Design and Implementation of a Secure Modbus Protocol Critical Infrastructure Protection III" vol. 311 pp. 83-96 2009.

[9] H. Alzaid et "Mitigating Sandwich Attacks against a Secure Key Management Scheme in Wireless Sensor Networks for PCS/SCADA" Proc. 24th Int'l. Conf. Advanced Information Networking and Applications vol. 2010 pp. 859-65.