Development of Secure Examination Marking System

Nang Thidar Htwe, Tin Mar Kyi
Computer University (Loikaw)
nangthidarhtwe@gmail.com, tinmarkyi@gmail.com

Abstract

This paper describes a potential vulnerability that allows a less-than brute force regeneration of the secret enrolled marks data. Protection of data during transmission in storage may be necessary to maintain the confidentiality and integrity of the information represented by the data. In order to secure and trust the student's examination result, this system is developed by using Hash function named Message Digest function (MD5) and Data Encryption Standard (DES) algorithm. This system provides a broad of the subjects and develops for secure exam marks transfer within the context of a total security program and network access controls.

Keywords: Data Encryption Standard (DES), Message Digest (MD5**).**

1. Introduction

The course work and content of education catered and technology has provided many teaching aids. However, the age process of the system hall still remains and in many circumstances a barrier to potential students. An exam solution overcomes obstacles and provides opportunities for individual to gain qualifications [2].

Nowadays, an education plays as an important role. The responsibility of schools and universities are to improve the ability of students. The examination process of collecting marking and certifying is sometimes bureaucratic and error prone. When the student marks has transported to other schools or universities, marks are need to be secure. The fundamental method for this has been with the use of encryption.

There are many aspects of security and many applications, ranging from secure exam marks commerce and marks sent communication and protecting attacks. One essential aspect for secure exam marking result that while cryptography is necessary for secure exam marks communication. Cryptography provides the basics for authentication of messages as well as their security and integrity carefully designed security protocols are required to exploit it [3].

Therefore, in this system, we will use the file to keep students results and encrypted roll number and marks. This simple application used cryptographic Hash functions named Message Digest (MD5) algorithm and to encrypt data file using Data Encryption Standard (DES) algorithm before it can be sent the students exam marks.

2. Related Work

This paper can provide the secure way for student's exam mark data transfer. Varieties of methods have been used to hide information by the use of encryption. Nowadays, education plays as an important role. Thus, the students' marks must be taken care of the security. Because marks are important for the students. When the result of student mark have been transported, mark are needed to be secure. Therefore, cryptosystems are the methods an functions used to encrypt and decrypt data for the students's marks file.

This paper applies DES algorithm and message digest MD5 algorithm, so, the user can be achieved fast encryption, speed and solved the attack problems for more seucre exam mark transfer. Then, it is commonly used for file integirty checking and to produce the two messages have the same message digest. So, this paper develops for the student's marks result to be secure by using the method of data encryption standard (DES) algorithm and message digest (MD5) alogrithm functions.

3. Background

Cryptography has become a widely used tool in communications, computer networks, and computer security generally. Cryptography is a physical process that scrambles information by rearrangement and substitution of content, making it unreadable to anyone except the person capable of unscrambling it. With the shear volume of sensitive Internet transactions that occur daily, the benefit of securing information using cryptographic processes becomes a major goal for many organizations. Since no cryptographic system is foolproof, the idea is to make the cost of acquiring the altered data greater than the potential value gained [4]. Essentially, it becomes an issue of deterrence.

All cryptographic processes have four basic parts:

Plaintext: This is the original intelligible message or data that is fed into the algorithm as input.

Cipher text: This is the scrambled message produced as input. It depends on the plaintext and key. Cipher text is an apparently random stream of data, and is unintelligible.

Key: A mathematical value, formula or process that determines how plaintext message is encrypted or decrypted. The key is only way to decipher the scrambled information.

Cryptographic algorithm: This is the converting plaintext to cipher text using cryptographic algorithm is called encryption and converting cipher text back to plaintext using the same cryptographic algorithm is called decryption [4].

3.1 Encryption

Encryption is the process of converting a plaintext message into cipher text that can be decoded back into the original message. An encryption algorithm along with a key is used in the encryption and decryption of data.

3.2 Decryption

Decryption is the same as an encryption algorithm but sub keys are applied in reverse order.

3.3 Attacks and threats

The main goal of security is to restrict access to information and resources to just those principal that are authorized to have access [5]. Security threats fall into three broad classes:

Leakage the acquisition of information by un-authorized recipients.

Tampering: the unauthorized alteration of information. Method of attacks could be classified according to the way in which a channel is misused.

Eavesdroppin*g*: obtaining copies of message without authority.

Masquerading: sending or receiving messages using the identity of another principal without their authorities.

Message tampering: interception message and altering their contents before passing them on to the intended recipient. The man-in-the middle attack is a form of message tampering in which an attacker interprets the very first message in an exchange of encryption key to establish a secure channel [5].

3.4 Cryptographic algorithm

There are several ways of classifying cryptographic algorithms. They will be categorized based on the number of keys that are employed for encryption and decryption, and further defined by their application and use. There are several ways of classifying cryptographic algorithms.

Secret key cryptography (SKC): uses a single key fro both encryption and decryption.

Public-key cryptography (PKC): uses one key for encryption and another for decryption.

Hash functions: uses a mathematical transformation, to irreversibly "encrypt" information.

4. Data encryption standard (DES)

The Data Encryption Standard (DES) provides a complete description of a mathematical algorithm for encrypting (enciphering) and decrypting (deciphering) binary coded information. DES is a symmetric block-cipher that transforms 64 bits data blocks using a 56 bits shared secret key, involving 16 rounds of permutation and substitution [7]. It has been found that the number of rounds is exponentially proportional to the amount of time required to find a key using a brute-force attack. Therefore, as the number of rounds increases, the security of the algorithm increases exponentially.

4.1 Encryption and decryption with DES

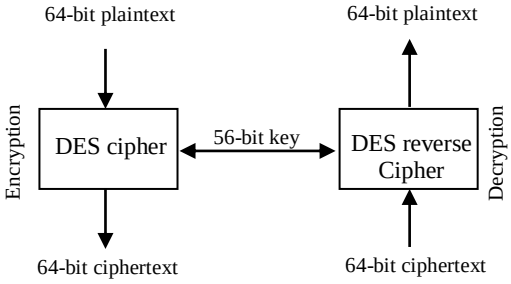

Figure 1 Encryption and decryption with DES

At the encryption site, DES takes a 64-bit plaintext and creates a 64-bit ciphertext, ant the decryption site, DES takes a 64-bit ciphertext and creates a 64-bit block of plaintext. The same 56-bit cipher key is used for both encryption and decryption.

4.2 DES structure

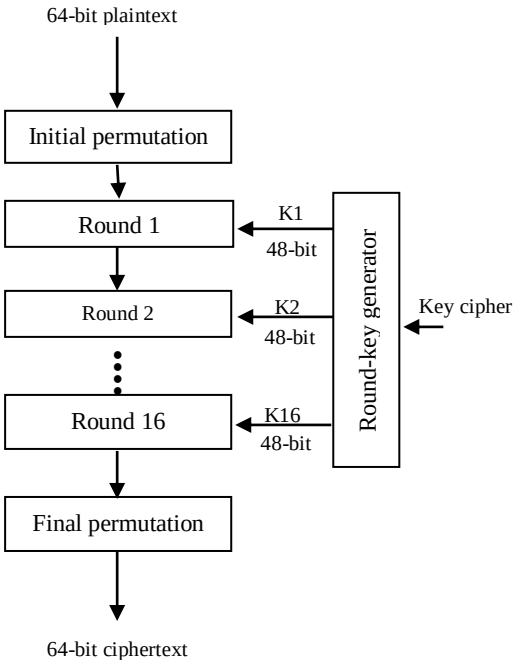

Figure 2 Structure of DES

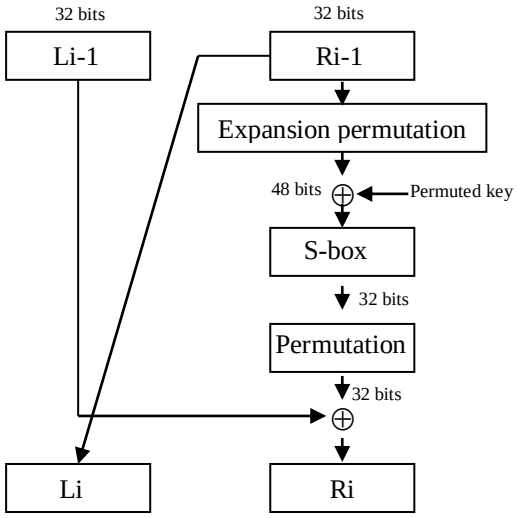

Figure 3 A round in DES

The round takes L_{i-1} and R_{i-1} from initial permutation box and creates Li and Ri, which go to the next round. Each round has two cipher elements. Each of these elements is invertible. It swaps the left half f the text with the right half. The mixer is invertible because of XOR operation.

5. Hashing

Producing hash values for accessing data or for security. A hash value also called a message digest is a number generated form a string of text. The hash is substantially smaller than then text itself, and is generated by a formula in such a way that is unlikely that some other text will produce the same hash value.

Hashes play a role in security system where there are used to ensure that transmitted message have not been tampered with. The sender generates a hash of the message, encrypts it, and sends it with the message itself. The recipients then decrypt the message and hash, produce another hash from the received message, and compare the two hashes. If they are the same, there is a very high probability that the message was transmitted [6]. To make hash function work, they should have two properties [1];

- Given a particular message digest, it should be very difficult to find an input that has the same message digest.
- It should be very difficult to find two inputs that have the same message digest.

5.1 Message digest function

Message digest functions distill the information contained in a file (small or large) into a single large number, typically between 128 and 256 bits in length. Message digests are also called one-way hash functions [1] because they produce values that are difficult to invert, resistant to attack, mostly unique, and widely distributed. Many message digest functions proposed and are in use today. Here are just a few like HMAC, MD2, MD4, MD5, SHA-1. In this article, one of the widely used is MD5 digest function.

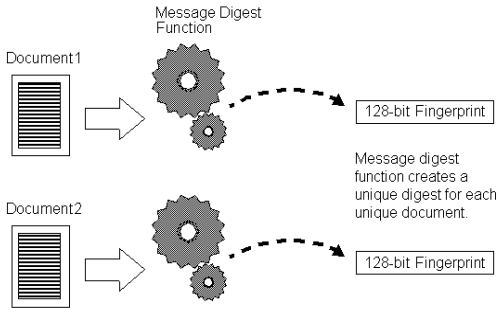

Figure 4 Message digest function

5.2 Message digests (MD5)

In cryptography, MD5 is a widely used cryptographic hash function with a 128-bit hash value. MD5 has been employed in a wide variety of security applications, and is commonly used to check the integrity of files. An MD5 hash is typically expressed as a 32 digit hexadecimal number. The MD5 algorithm is also known to be secure. The function is also known to be collision-free. The closet attack found was the ability to

generate a pseudo-collision operation. However, this does not seem to cause any notable risk.

5.3 Algorithms

Step 1: Append padding bits
Step2: Append length
Step3: Initialize MD buffer
Step4: Process manage in 16 word blocks
Step5: Output

- MD5 process variable length message into fixed length output 128 bit.
- Calculates a cryptographic hash or secure checksum of plaintext. The hash is appended to the message before encryption.
- On decryption, the hash is recomputed from the resulting plaintext.
- The plaintext hash decrypted to a different value from before, the hash computation leads to a different value [8].
- If the value does not match, the expected one appended to the message, and can therefore tell that tampering has occurred [8].

6. System flow chart

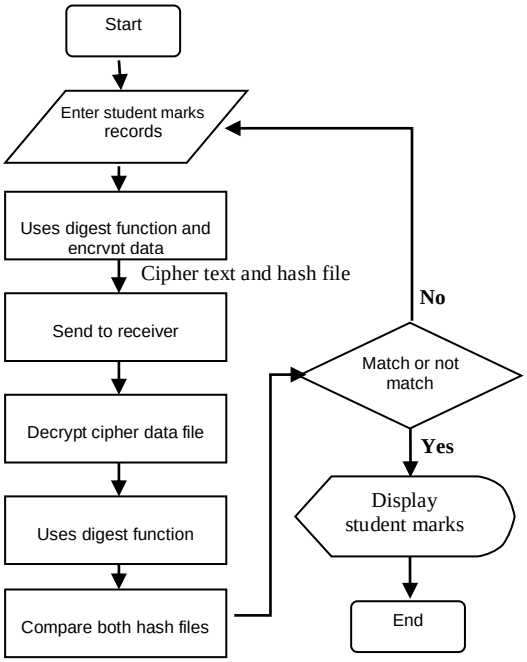

Figure 5 System flow chart for the system

The system flow chart includes encryption and decryption and message digest components. The encryption and decryption component are DES file component and MD5 hash function component. The sender needs to perform the file encryption and file digestion. The receiver needs to perform the file decryption and compare digest files. To encrypt and digest file, the sender needs to perform the following steps;

- Digest the user selected file by using MD5 algorithm.
- Save the digest file and encrypt the user selected file with DES (Symmetric algorithm).
- Send the encrypted file and digested file to the receiver pass through the insecure channel.
- To decrypt the file, the receiver needs to perform the following steps;
- Decrypt the file with DES (Symmetric) key algorithm.
- Save the decrypted file and digest with MD5 (Hash function) algorithm.
- Then, compares both digest files are the same.

6.1 Procedures for secure exam mark system

- Firstly, the sender entered the student's exam marks results.
- Then, sender made digest file by using MD5 algorithm and use DES algorithm to encrypt the student's exam marks. Hash file and ciphertext are appeared.
- And then, the sender use remote host IP address to send both ciphertext and hash file to the receiver.
- When the receiver received both files, receiver decrypts the ciphertext by using DES algorithm. The plaintext can be obtained.
- Again, the receiver digests the plaintext file by using MD5 algorithm. Then compare the two hash files, are they match or do not match.
- If the two hash files are match, receiver assumes that files hash not occurred tampered attacks and files are secure and valid.

6.2 Advantages of the system

It is commonly used for file integrity checking and as a message digests in digital signatures schemes. It is computationally infeasible to produce two message have the same message digest. Prevent unauthorized gain of information, i.e. loss of confidentiality and avoid unauthorized modification information, and then keep away from unauthorized impairment of functionality. It is used to encrypt high-volume high-speed transmission of confidential data. This is of considerable importance especially as such an encryption scheme can easily be implemented on the chip thereby reducing the cost drastically.

6.3 Proposed system

The system is implemented over the symmetric cryptosystem, provides robustness and adaptability, and protects the exam marking transactions. By using DES algorithm, it can support the effective of encryption technique and

developed for exam marks transfer. Then, it can defend tampering attackers' disturbance due to message digest named MD5 functions.

6.4 Limitations

It can only be supported the cryptography portion of security in distributed system. The security of the system depends on the key security. It is then allows only text file with the format of the system. It cannot be used with other applications text files. Therefore, this paper should be limited in use.

7. Conclusion

The performance of cryptography and digest system is to make it possible for two people to exchange a message in such a way that other people cannot understand the message. The system is implemented the demonstration of DES and MD5 algorithms, the performance of Symmetric cryptography due to DES algorithm is faster and support the effective encryption techniques. On the other hand, message digest function named MD5 algorithm is more efficient and create with the same checksum file. MD5 cannot protect against some forms of malicious tampering. Therefore, the system can take their advantages and can support an effective encryption and compression technique for transporting of student's examination marks results.

REFERENCES

[1] Arnoud Engelfriet, "Cryptographic hash functions" October 2005 http://www.iusmentis.com/technology/hash func-tions

[2] http://www.exsol.org/contents.html

[3] Gray C. Kessler, "An Overview of cryptography", May 1998

[4] http://www.ssh.fi/tech/crypto/intro.html#algorihm

[5] George Koulouris, Jean Doll more Tim Kind berg, "Distributed system concepts and design", third edition

[6] http://www.weboedia.com/TERM/hashing

[7] Matthew Fischer, "How to implement data encryption standard (DES)", version 1.24, November 1995 http://www.itl.nist.gov/dipspubs/fip46-2.html

[8] http://www.faqs.org/rfcs/rfc1321.html