Encryption and Preserving Data Integrity Scheme for Communication Exhausting MD5 Cryptographic Procedures

Pushpendra Kumar Verma
Assistant Professor, Computer Science department,
Swami Vivekanand Subharti University, Meerut, Uttar Pradesh, INDIA.
Email - dr.pkverma@gmail.com

Abstract: *Data security and information attracts a lot of people's attention ensures the authenticity of data or documents still Awake, this problem is so urgent to and touching various fields including secure communication channels, Strong and reliable data encryption techniques are needed to maintain the database. Message Digest 5 (MD) is a cryptographic method that uses a key such as a password in the process of encryption and Use the same key to perform the decryption process so that the same document will be generated With the original document. The plaintext data that has been encrypted will result in a chipertext that does not can be read by others. Chipertext is what will be sent to a second party so it will have Reliable secrecy. The resulting chipertext data will vary according to key data input Password provided. This system is created with Visual Basic.Net preemptive language.*

Key Words: *Md5, Cryptography, Hash Function, Data Integrity, Collision, Algorithm, Digital Signature*

1. INTRODUCTION:

The development of information technology today has an effect on almost all aspects of human life. Currently the Internet as ignores geographical boundaries of a country, not a difficult thing for a person to communicate remotely, transmits the data, searching for information and so on. All this can be done with the Internet in a fast, efficient and relatively inexpensive. But on the other hand, it turns out the Internet is a path that is not too safe because it is a common communication medium that may be useful late freely by anyone so it is prone to interception of information by parties that are not valid. Therefore the issue of safety, comfort and authorization dal a m surfing a crucial issue that remains to this day a warm conversation. Questions that arises, whether the transaction via the Internet can be secured. Is the data transmitted via the Internet to the proper destination without being detected unwanted? How to prevent the interception of information? How can someone steal anticipates the data?

Many methods can be done to answer the above questions. One of them with a method of encoding or better known as the cryptographic methods. There are so many methods of encryption or cryptographic methods developed by experts in cryptography to date. This was done due to the tapper and information thieves or better known as cracker more reliable in penetrating a system to explore the various kinds of information. Therefore, in order to fight against the heinous act, cryptography experts continue to develop this ode met on an ongoing basis. Lots of encoding methods that have been created by experts in cryptography world, call it Algorithm DES, 3DES algorithm, Algorithm IDEA, Blowfish algorithm, Algorithm RSA, algorithm MD4, MD5 Algorithm, Algorithm SHA-1 algorithm McEliecce and so forth. Algorithms above have been tested for their ability by expert's cryptography, but not all of the above cryptographic methods survive attacks from eavesdropper's information or in terms of cryptography is often referred to cryptanalyst. Call it the DES algorithm, had lasted long enough that for 20 years finally be willing to be crack in just 3,5jam at a cost of 1 million US dollars in 1993. But expert's cryptography is not silent, because after that the experts cryptography develop new variants of DES algorithms such as 3DES algorithm, Algorithm RDES and so forth.

This paper will discuss one among much powerful cryptography that is still strong enough to stem the attacks from the cryptanalyst, the method of cryptographic Message Digest algorithm 5 (MD5). In addition to its cryptographic methods have not been able in the break by cryptanalyst, this paper discusses cryptographic algorithms MD5 because this is a new variant after the algorithm MD2 and MD4 algorithms that are considered up to date for today.

1.1 Research purposes

Making paper intends to analyze the process of encoding a message and reopen the encoding process in cryptography, particularly the MD5 cryptographic algorithm. Expected by this paper path more Internet users to be extra careful in the use of this public path. For security method can use the method MD5 cryptographic algorithms are discussed in detail in this paper.

1.2 Research Method

In making this paper, the research methods that I use are the method of literature. I use this method because I think the literature method is the most appropriate method to use. Moreover, to add weight to information that can be absorbed from these papers, I took some references from the books discuss the MD5 cryptographic algorithm.

2. THEORY:

2.1 Terminology Cryptography

The word cryptography is derived from the Greek crypto *(hidden* or *secret)* and graph *(writing)* so that means the *secret writing*. In terms of cryptography is defined as a science and an art to maintain the confidentiality of messages (data or information) who has an idea, a way to disguise (scrambles) into a form that cannot be understood using a specific algorithm.

In the science of cryptography a message to be suppressed or encoded called the *plaintext,* while the message that was encrypted so no meaningful again aiming for a message cannot be read by unauthorized parties called *ciphertext*. Then there is the term in the term in the science of cryptography encryption and decryption. Encryption is the process of encrypting *plaintext* into *ciphertext*. While the process of restoring the original plaintext into *ciphertext* is referred to as description. Here is a general scheme of a cryptographic encryption:

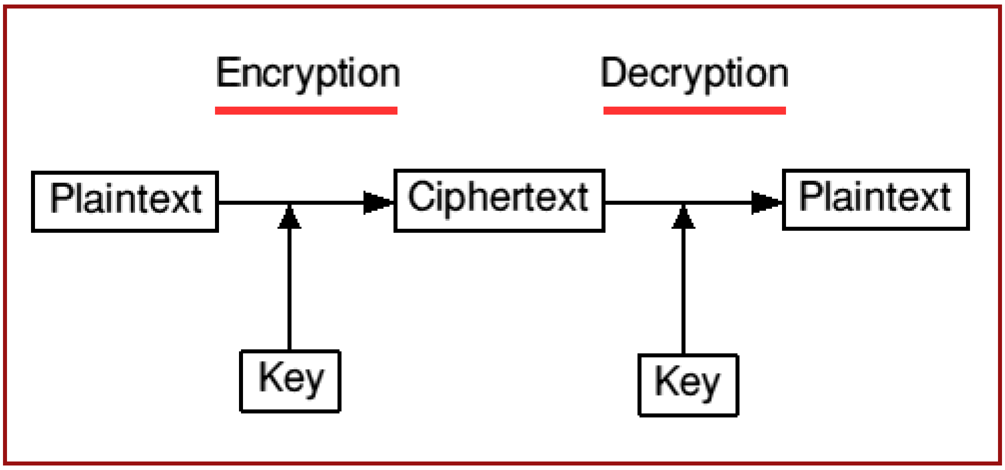


Figure 1: Schematic Cryptography

2.2 History of Cryptography

Science of cryptography allegedly swampy l from 4000 years ago, the nation recorded using the Egyptian *hieroglyph* which is not standard in writing a message Later, around the year 400SM in the days of ancient Greece, used by soldiers Sparta cryptography to transmit military messages by using a tool called *scytale*. This tool is a long ribbon of papyrus leaves plus a piece of the cylinder, the message is written horizontally or line per line. If the tape is removed, then the letters in it has been arranged to form a secret message. To read the message, the recipient must wind the tape back into the cylinder with a diameter equal to the diameter of the cylinder sender.

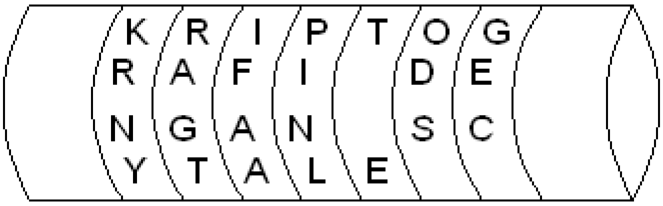


Figure 2: scytale

Since ancient science of cryptography is used in various aspects of life. For example in India, formerly used by a cryptographic lovers (lover) to communicate without being known to others. This evidence is found in the book Kama sutra which recommends that women should learn the art will understand the cipher.

P Then there are the 17th century, the history of cryptography ever recorded casualties in the UK. Queen Mary of Scotland, was beheaded after his secret messages from behind prison (an encrypted message that it plans to kill Queen Elizabeth I) successfully solved by Thomas Phelippes, a code breaker.

Science of cryptography is also used in World War II, Nazi German government makes encryption machine called Enigma. Then not long ago Enigma cipher successfully solved by the allies, the success of solving Enigma pointed out as factors that shorten World War II.

Of some historical quote above, it can be seen that the science of cryptography is helpful especially in the military. This time as the development of human civilization and the entry age to the information age, the science of cryptography also used to secure traffic information, especially in the public network or the Internet.

Parent of cryptography is the science of mathematics, especially algebra theory that men became the basis of the science of numbers. Therefore cryptography is growing rapidly when the computer was invented. Because the present invention allows a computer to do the calculations was complicated and complex in a relatively short time, something that previously could not be done. Hence was born the many theories and data encryption algorithm increasingly complex and difficult to solve.

2.3 Interest Cryptography

In general purpose cryptographic knowledge created is to keep a message that cannot be read by those who are not legitimate. Guided by the common goal, there are four fundamental objective science of cryptography is used in the field of information security, namely:

a. **Secrecy** is a service that is used to keep the contents information from anyone except those having authority or a secret key to open / peel the information that has been encoded.

b. **Data integrity** is related to secure data from unauthorized changes. To maintain the integrity of the data, the system must have the ability to detect the manipulation of data by parties who are not entitled to, among other things insertion, deletion, and other data pen substitution into the actual data.

c. **Authentication** is associated with the identification / recognition, either as a whole system as well as the information itself. Two parties communicating must be introduced themselves. Information submitted via the canal must be authenticated authenticity, data contents, delivery time, and others.

d. **Non-repudiation** is an attempt to prevent the denial of shipments / creation of information by transmits / make.

2.4 Cryptanalysis

Cryptanalysis is an efforts carried out by someone to obtain information or data that has been encrypted. People doing cryptanalysis activities referred to *cryptanalyst.* There are five types of *cryptanalysis* following describes the five types of *cryptanalysis:*

types of attacks	To note *cryptanalyst*
Ciphertext-only	encryption algorithm *Ciphertext* will decrypted
known plaintext	encryption algorithm *Ciphertext* to be decrypted One or more pairs *plaintext-ciphertext* message
Chosen plaintext	encryption algorithm *Ciphertext* to be decrypted *Plaintext* chosen by *cryptanalyst,* along with his partner*ciphertext*
Chosen ciphertext	encryption algorithm *Ciphertext* to be decrypted *ciphertext* chosen by *cryptanalyst,* along with his partner *plaintext*
Chosen text	encryption algorithm *Ciphertext* to be decrypted *Plaintext* chosen by *cryptanalyst,* along with his partner *ciphertext* *Ciphertext* chosen by cryptanalyst, along with his partner plaintext

2.5 Cryptography classification

In terms of the development era science of cryptography is divided into two, namely the classical cryptography and modern cryptography.

2.5.1 Classical cryptography

Judging from its name of course classical cryptography is the beginning of the development of the science of cryptography. In this era of the development of cryptographic strength lies in the secrecy of the algorithm used, this type of algorithm called algorithm *restricted.* But amid *restricted* development algorithm found many weaknesses that are not relevant for the purposes of current information security. As for weaknesses *restricted* algorithm is as follows:

- *Restricted* algorithm is an algorithm that is confidential, so the ability of the algorithm was never tested by experts in cryptography and the impact on distrust of *the* user or *users* will be toughened.
- In the event of a leak secret algorithm, it should be created or developed new algorithms. The consequence is wastage costs due to the cost of making a new cryptographic algorithm are very expensive.

2.5.2 Modern cryptography

Modern cryptography developed to remedy some weaknesses possessed by previous cryptography classical cryptography. Contrary to classical cryptography, algorithms used in modern cryptography in an open or expected in other words known by general so as not confidential. This is done to cover the weaknesses of classical cryptography, so the algorithm of modern cryptography can be tested toughened by cryptography experts. Then where lies the power of modern cryptography? The cryptographic strength of the encryption key is based on secrecy. Based single key, modern cryptography is divided into two types: symmetric key cryptography and asymmetric key cryptography.

2.5.2.1 Cryptography Lock Symmetric

P No. cryptographic, encryption methods and descriptions using the same key. For example the encryption key is K, then the key description of the same with the encryption key, K.

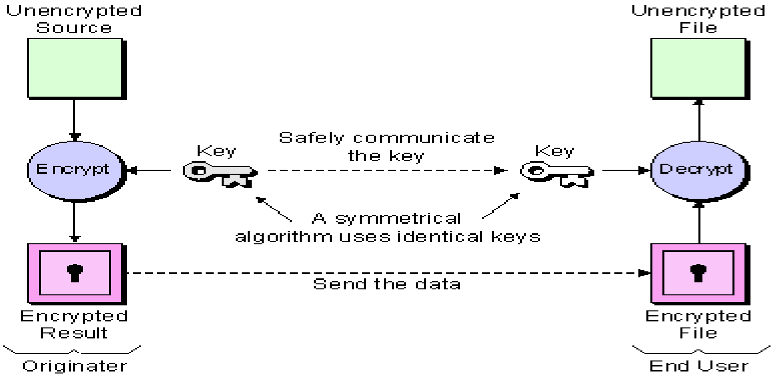


Figure 3: symmetric-key cryptography scheme

In symmetric key cryptography, to maintain the confidentiality of messages between the communicants we need a key for each partner communicant. So that for n communicant number of keys required is:

n (n-1)/2

Symmetric cryptography superiority lies in the speed encryption process or description. This is an added value for symmetric-key cryptography, because cryptography is usually applied in a network. In the science of the network is said that a good network is a network that has the most minimal delay time. Symmetric key cryptography so strongly supports the *statement.* And another advantage is the relatively resilient cryptographic chosen-plaintext attack because the key is confidential.

Key cryptography symmetry is not without weaknesses, constraints on the first cryptographic key management are located in a very tricky. The more communicant communicating the more keys required number of keys, for example, there are 1000 499 500 communicants are needed all key can communicate with each other communicants. With the keys as much as it would be very difficult to remember and maintain a secrecy. Then the second obstacle lies in the key distribution because it takes a dedicated channel to distribute keys. Key distribution cannot be done using the channel or medium that will be used communication, because in fact this is the path that should be secured.

There are several algorithms developed by experts in cryptography uses symmetric cryptography, among others:

- DES algorithm
- IDEA algorithm
- Blowfish algorithm
- RC2 algorithm

2.5.2.2 Cryptography Key Asymmetric

Asymmetric key cryptography uses different keys (key pairs) for the purposes of the encryption process and process descriptions. The key used in the encryption process is usually called the public key or the public key, while the keywords used in the description is usually referred to as the private key. The difference is very visible among key cryptography symmetry and key cryptography asymmetry lies in the nature of a key, the key cryptography symmetric key is private, while the cryptographic key asymmetry there are a couple of keys that have two different properties, namely the private key to the process decrypts and key public to encrypts process. Due to the nature of one of the public key cryptography asymmetric key cryptography is often referred to as public key algorithm.

Developed asymmetric key cryptography experts to overcome the difficulties of the distribution of cryptographic keys at key cryptography symmetric. Distribution of keys on a key cryptography asymmetry is very easy, because the key is pubic encryption or the public key distribution can be done anywhere on the track even though the path that you want to secure. The following encryption schemes and descriptions in asymmetric cryptography:

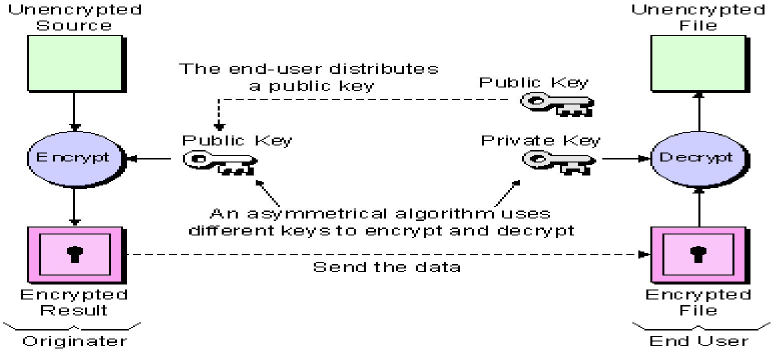


Figure 4: asymmetric key cryptography scheme

Cryptography is not without loopholes, because the encryption key is public then the cryptography is relatively weak against attacks cryptanalyst especially *chosen-plaintext* attack. Additionally, cryptography has other drawbacks in terms of speed. Asymmetric cryptography 1000 times slower than symmetric cryptography. The advantages of asymmetric key cryptography in addition to the key distribution is very easy key management is not complicated because each communicant just need a pair of keys (encryption and description), so it can be written to n communicant who communicate only in need n pairs of keys.

There are many algorithms developed by experts for key algorithm asymmetric cryptography, among others:

- RSA algorithm
- algorithms McEliece
- algorithm Rabin
- algorithm Knapsack
- algorithms LUC
- Algorithms El Gamal

To cover the shortfall from each other symmetric-key cryptography and asymmetric key cryptography, the cryptography experts to develop this merger of two methods of cryptography. Merging method is called Hybrid Cryptosystem. In this method, symmetric key algorithm used to secure messages or data to be transmitted. While the asymmetric key algorithm used to secure the keys from cryptographic process symmetry.

2.6 Hash functions

The hash function is a function that accepts any input *string* length and converts it to a fixed length output *string (fixed)* (generally much smaller than the size of the original *string). The hash* function can accept any input *string*. If the string stating the message (message), then any message M-size compressed by a hash function H by the equation:

$$\boxed{h = H(M)}$$

Exodus hash function is also called hash value (hash value) or a quick message (message digest) . In the above equation, h is the hash value or message digest of the function H to enter M. In other words. the hash function message compress any size whatever be the message digest size is always fixed (and shorter than the length of the original message).

The hash function used to verify a copy of data similarity n Data original premises. For example in a company, rather than sending a copy of the entire archive to a central computer (assuming the company is using a centralized database). Better send his *message digest.* If *message digest* an archived copy of the same as the *message digest* the original archive, the archive copy of the same with the records in the database.

The hash function is often referred to as *one- way* hash *function* for function works in one direction, that is the message that has been converted into *a message digest* cannot be restored into the original message. The properties of the hash function is as follows:

- *H* functions can be applied to any size data blocks only.
- *H* produces a value *(h)* with a fixed length *(fixed length output).*
- *H (x)* is calculated for each value of *x* is given.
- For every *h* generated, it is not possible to recover the value of *x* such that *H (x)* = *h.* That is why the function *H* is said to be a one-way *hash* function *(one-way hash function).*
- For any given *x, y* ^{1} not likely to find *x* such that *H (y)* = *H (x).*
- Not likely to find *a* pair *x* and *y* such that *H (x)* = *H (y).*

There are several cryptography experts developed using a cryptographic hash function, such as:

- MD2 algorithm
- algorithms MD4
- MD5 algorithm
- algorithm SHA
- Algorithm RIPE-MD160
- Announcements

Here are some other names of the hash function:

- the function of compression / contraction (compression function)
- Print-finger *(fingerprint)*
- *cryptographic checksum*
- *message integrity check* (MIC)
- *manipulation detection code* (MDC)

3. DISCUSSION:

3.1 Method of P encryption PM With Cryptography A MD5 algorithm

MD5 algorithm is an algorithm that uses one-way hash function created by Ron Rivest. The algorithm is an extension of previous algorithms is algorithms MD2 and MD4 algorithms because both algorithms have successfully attacked the *cryptanalyst.*

How it works is the MD5 cryptographic algorithm accepts input in the form of a message with any size and produces a *message digest* which has a length of 128 bits. The following illustration of the creation of message digests on cryptographic algorithms MD5:

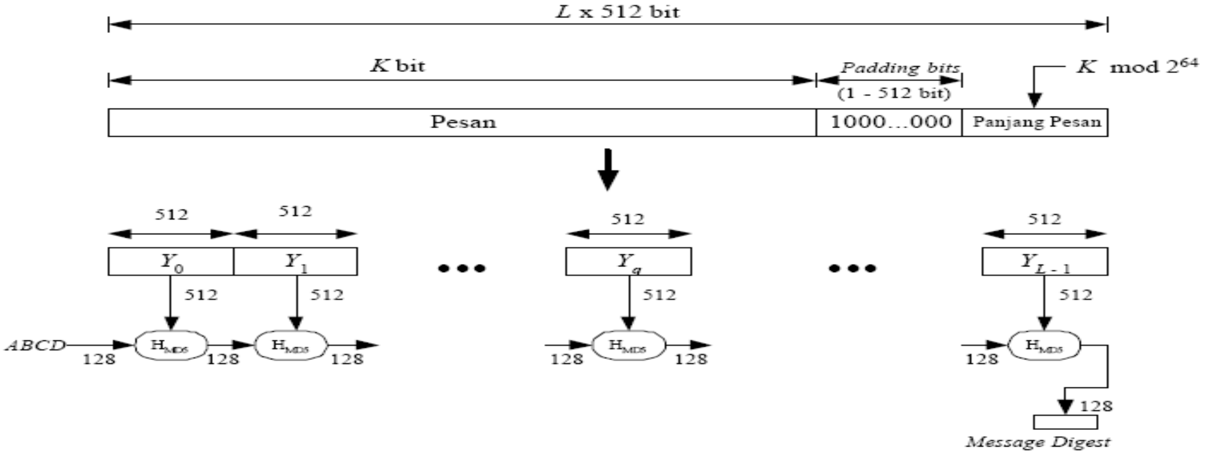


Figure 5: Making the MD5 message digest algorithm

Judging from the picture above, an outline of the manufacturing *message digest* is made through four steps:

1. Extra bit encryption

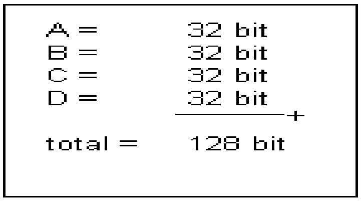
The first process is done is add a message with the number of bits booster so that the message length (in bits) is congruent to 448 modulo 512. This means that after adding bits booster, now the message length is 64 bits less than a multiple of 512. Things to remember is the number 512 appear because the MD5 algorithm to process messages in blocks 512.

If there is a message with a length of 448 bits, then the message will still be added with the bits of a booster. Messages will be added to 512 bits to 96 bits. So long bits wedge is between 1 and 512. Then another thing to note is that the bits booster consists of a binary 1 followed by the remaining bits 0.

2. Extra length value original message

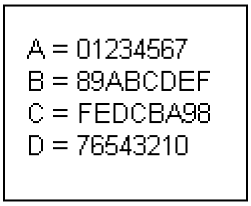
then the next process is coupled with a message stating 64 bit length original message. If the message length is greater than 2^{64} then taken is the length of modulo 2^{64}. in other words, if initially the message length equal to K bits, then 64 bits, written stating K modulo 2^{64}. so that after the second process is completed, the current message length is 512 bits.

3. Initialize MD buffer At the MD5 algorithm takes four buffer or buffers, sequentially fourth buffer names are named A, B, C and D. Each buffer has a length of 32 bits. So that the total length:



A =	32 bit
B =	32 bit
C =	32 bit
D =	32 bit +
total =	128 bit

4. This buffer holds fourth intermediate results and final results. Each buffer is initialized with the values (in Hexadecimal notation) as follows:



A = 01234567
B = 89ABCDEF
C = FEDCBA98
D = 76543210

5. Processing messages within a block size of 512 bits

Be very next process is divided into L pieces of message blocks, each of which length is 512 bits (Y_0 to Y_{L-1}). After that each block of 512 bits processed together with the MD buffer which generates output of 128 bits, and it is called H_{MD5}. Here is an overview of the process H_{MD5}:

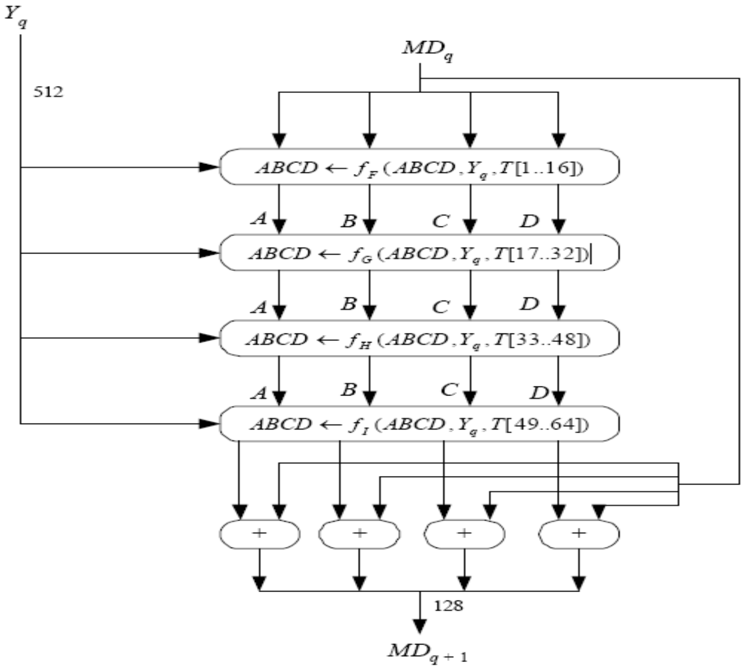
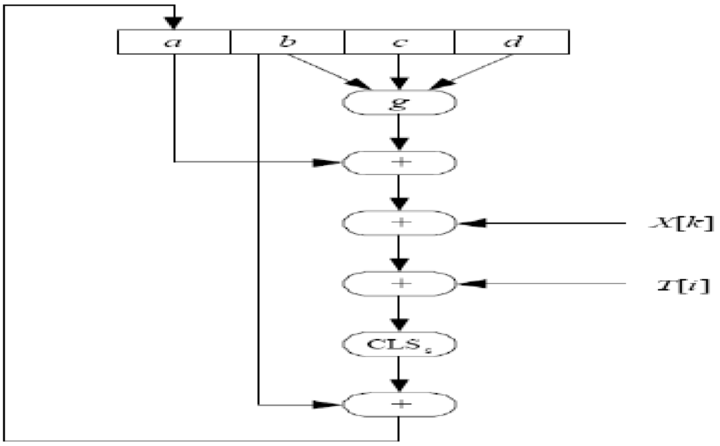

Y_q
512
MD_q
$ABCD \leftarrow f_F(ABCD, Y_q, T[1..16])$
A
B
C
D
$ABCD \leftarrow f_G(ABCD, Y_q, T[17..32])$
A
B
C
D
$ABCD \leftarrow f_H(ABCD, Y_q, T[33..48])$
A
B
C
D
$ABCD \leftarrow f_I(ABCD, Y_q, T[49..64])$
+
+
+
+
128
MD_{q+1}

Figure 6: block 512 bit Processing (Process H MD5)

From the picture above us can see that the process H $_{MD5}$ consists of 4 pieces rounds, and each round perform basic MD5 operation 16 times. Where each basic operation wears an element T. Thus each round table elements wear 16 T.

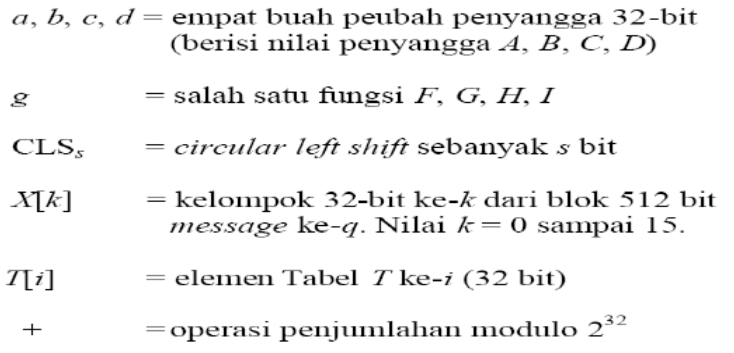
I n Figure 6, block 512 Y $_q$ states q bits of all of the messages that have been added with the bits of a booster in the first process and additional 64 bit length value of the original message in the process. MD $_q$ is 128 bit *message digest* value of the H $_{MD5}$ to-q. At the beginning of the process, an initial value buffer containing MDQ MD. Then the function f $_{F,}$ f $_{G,}$ f $_H$ and f $_I$ in the picture, each containing 16 times the basic operations of the input, each of the basic operations use element T. The following table illustrated the basic operation MD5:



The basic operation is shown in the image above MD5 can be written by the following equation:

$$\boxed{a \leftarrow b + \mathrm{CLS}_s(a + g(b, c, d) + X[k] + T[i])}$$

Where



a, b, c, d = empat buah peubah penyangga 32-bit (berisi nilai penyangga A, B, C, D)

g = salah satu fungsi F, G, H, I

CLS$_s$ = *circular left shift* sebanyak s bit

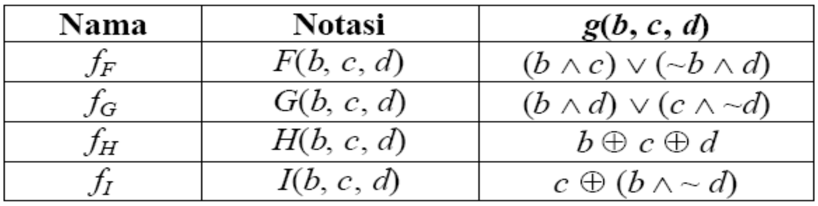
$X[k]$ = kelompok 32-bit ke-k dari blok 512 bit *message* ke-q. Nilai $k = 0$ sampai 15.

$T[i]$ = elemen Tabel T ke-i (32 bit)

$+$ = operasi penjumlahan modulo 2^{32}

Function f F, f G, f H and f I is a function to manipulate inputs a, b, c, and d with a 32-bit size Each function can be seen in Table 1 below:

Table 1 Basic functions MD5

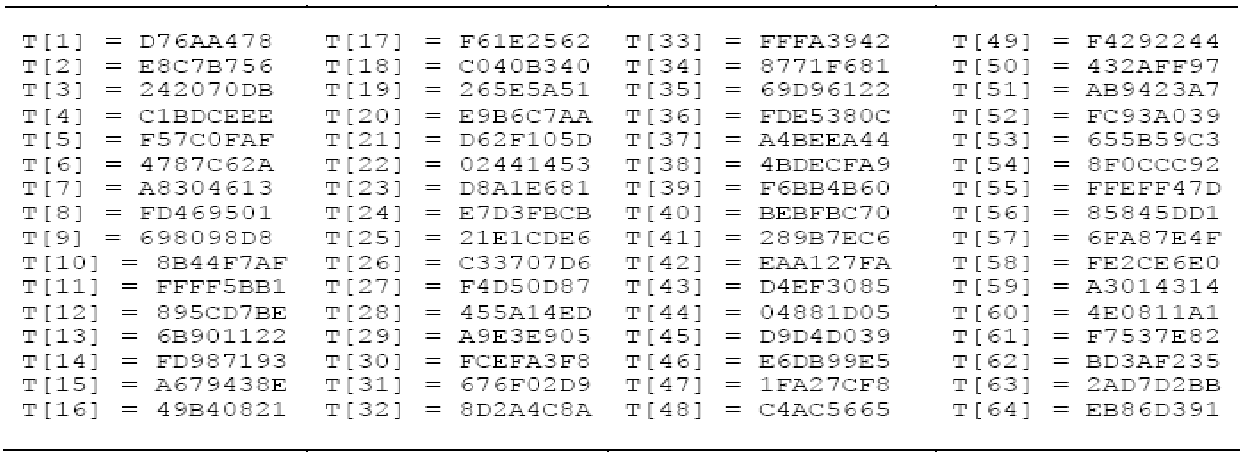


Nama	Notasi	$g(b, c, d)$
f_F	$F(b, c, d)$	$(b \wedge c) \vee (\sim b \wedge d)$
f_G	$G(b, c, d)$	$(b \wedge d) \vee (c \wedge \sim d)$
f_H	$H(b, c, d)$	$b \oplus c \oplus d$
f_I	$I(b, c, d)$	$c \oplus (b \wedge \sim d)$

A sequential logic operator AND**, OR, NOT and XOR denoted b □, □, ~, □**

Then the value of T [i] can be seen in the table below. These are organized by function 2 ^{32} x abs (sin (i)), i in radians.

Table 2. Value T [i]



T[1] = D76AA478	T[17] = F61E2562	T[33] = FFFA3942	T[49] = F4292244
T[2] = E8C7B756	T[18] = C040B340	T[34] = 8771F681	T[50] = 432AFF97
T[3] = 242070DB	T[19] = 265E5A51	T[35] = 69D96122	T[51] = AB9423A7
T[4] = C1BDCEEE	T[20] = E9B6C7AA	T[36] = FDE5380C	T[52] = FC93A039
T[5] = F57C0FAF	T[21] = D62F105D	T[37] = A4BEEA44	T[53] = 655B59C3
T[6] = 4787C62A	T[22] = 02441453	T[38] = 4BDECFA9	T[54] = 8F0CCC92
T[7] = A8304613	T[23] = D8A1E681	T[39] = F6BB4B60	T[55] = FFEFF47D
T[8] = FD469501	T[24] = E7D3FBCB	T[40] = BEBFBC70	T[56] = 85845DD1
T[9] = 698098D8	T[25] = 21E1CDE6	T[41] = 289B7EC6	T[57] = 6FA87E4F
T[10] = 8B44F7AF	T[26] = C33707D6	T[42] = EAA127FA	T[58] = FE2CE6E0
T[11] = FFFF5BB1	T[27] = F4D50D87	T[43] = D4EF3085	T[59] = A3014314
T[12] = 895CD7BE	T[28] = 455A14ED	T[44] = 04881D05	T[60] = 4E0811A1
T[13] = 6B901122	T[29] = A9E3E905	T[45] = D9D4D039	T[61] = F7537E82
T[14] = FD987193	T[30] = FCEFA3F8	T[46] = E6DB99E5	T[62] = BD3AF235
T[15] = A679438E	T[31] = 676F02D9	T[47] = 1FA27CF8	T[63] = 2AD7D2BB
T[16] = 49B40821	T[32] = 8D2A4C8A	T[48] = C4AC5665	T[64] = EB86D391

As previously explained that the function f $_{F,}$ f $_{G,}$ f $_{H}$ and f $_{I}$ do 16 times the basic operations. Suppose the following notation:

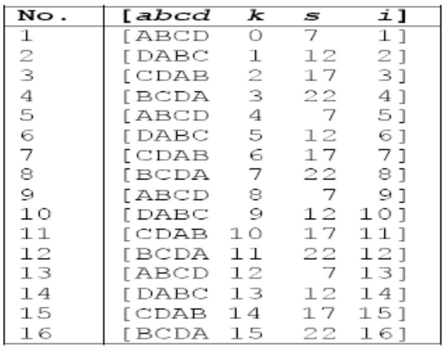
$$[abcd \quad k \quad s \quad i]$$

Stating operation

$$a \leftarrow b + ((a + g(b, c, d) + X[k] + T[i]) <<< s)$$

for operation above, <<< s symbolize operation circular left shift of 32 bits, the basic operations on each rotation can be tabulated as follows:- 1st round: 16 times the basic operations with g (b, c, d) - F (b, c, d), can be seen in the following table:

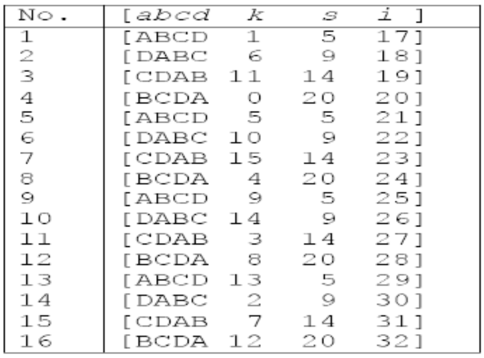
Table 3 details the operation on the function F (b, c, d)



No.	[abcd	k	s	i]
1	[ABCD	0	7	1]
2	[DABC	1	12	2]
3	[CDAB	2	17	3]
4	[BCDA	3	22	4]
5	[ABCD	4	7	5]
6	[DABC	5	12	6]
7	[CDAB	6	17	7]
8	[BCDA	7	22	8]
9	[ABCD	8	7	9]
10	[DABC	9	12	10]
11	[CDAB	10	17	11]
12	[BCDA	11	22	12]
13	[ABCD	12	7	13]
14	[DABC	13	12	14]
15	[CDAB	14	17	15]
16	[BCDA	15	22	16]

Round 2: 16 times the basic operations with g (b, c, d) - G (b, c, d), can be seen in the following table:

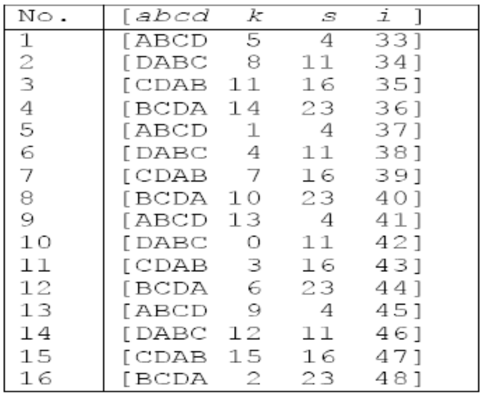
Table 4 details the operation on the function G (b, c, d)



No.	[abcd	k	s	i]
1	[ABCD	1	5	17]
2	[DABC	6	9	18]
3	[CDAB	11	14	19]
4	[BCDA	0	20	20]
5	[ABCD	5	5	21]
6	[DABC	10	9	22]
7	[CDAB	15	14	23]
8	[BCDA	4	20	24]
9	[ABCD	9	5	25]
10	[DABC	14	9	26]
11	[CDAB	3	14	27]
12	[BCDA	8	20	28]
13	[ABCD	13	5	29]
14	[DABC	2	9	30]
15	[CDAB	7	14	31]
16	[BCDA	12	20	32]

3rd round: 16 times the basic operations with g (b, c, d) - H (b, c, d), can be seen in the following table:

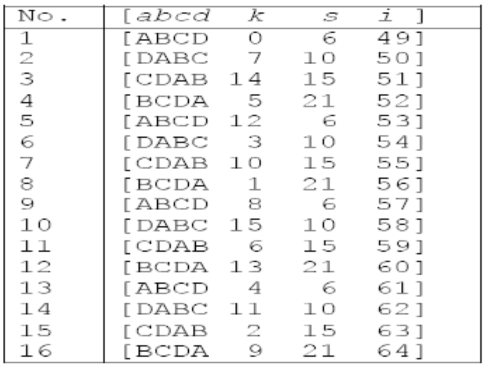
Table 5 details of operation on the function H (b, c, d)



No.	[abcd	k	s	i]
1	[ABCD	5	4	33]
2	[DABC	8	11	34]
3	[CDAB	11	16	35]
4	[BCDA	14	23	36]
5	[ABCD	1	4	37]
6	[DABC	4	11	38]
7	[CDAB	7	16	39]
8	[BCDA	10	23	40]
9	[ABCD	13	4	41]
10	[DABC	0	11	42]
11	[CDAB	3	16	43]
12	[BCDA	6	23	44]
13	[ABCD	9	4	45]
14	[DABC	12	11	46]
15	[CDAB	15	16	47]
16	[BCDA	2	23	48]

round 4: 16 times the basic operations with g (b, c, d) - I (b, c, d), can be seen in the following table:

Table 6 details the operation on the function I (b, c, d)



No.	[abcd	k	s	i]
1	[ABCD	0	6	49]
2	[DABC	7	10	50]
3	[CDAB	14	15	51]
4	[BCDA	5	21	52]
5	[ABCD	12	6	53]
6	[DABC	3	10	54]
7	[CDAB	10	15	55]
8	[BCDA	1	21	56]
9	[ABCD	8	6	57]
10	[DABC	15	10	58]
11	[CDAB	6	15	59]
12	[BCDA	13	21	60]
13	[ABCD	4	6	61]
14	[DABC	11	10	62]
15	[CDAB	2	15	63]
16	[BCDA	9	21	64]

After the fourth round, a, b, c and d are added to the A, B, C and D were subsequently algorithm will proceed to the next data block (Y q + 1). The output end of the MD5 algorithm is the result of splicing bits in A, B, C and D

From the description above, in general the MD5 hash function can be written in mathematical terms as follows:

$$\boxed{MD_0 = IV}$$

$$\boxed{MD_{q+1} = MD_q + f_I(Y_q + f_H(Y_q + f_G(Y_Q + f_F(Y_q + MD_q))))}$$

$$\boxed{MD = MD_{L-1}}$$

Where

IV = *initial vector* dari penyangga ABCD, yang dilakukan pada proses inisialisasi penyangga.
Y_q = blok pesan berukuran 512-bit ke-q
L = jumlah blok pesan
MD = nilai akhir *message digest*

To be more easily understood, the following examples of applying the MD5 cryptographic message that want to keep private. Suppose there is a file with the name duo.txt as follows:

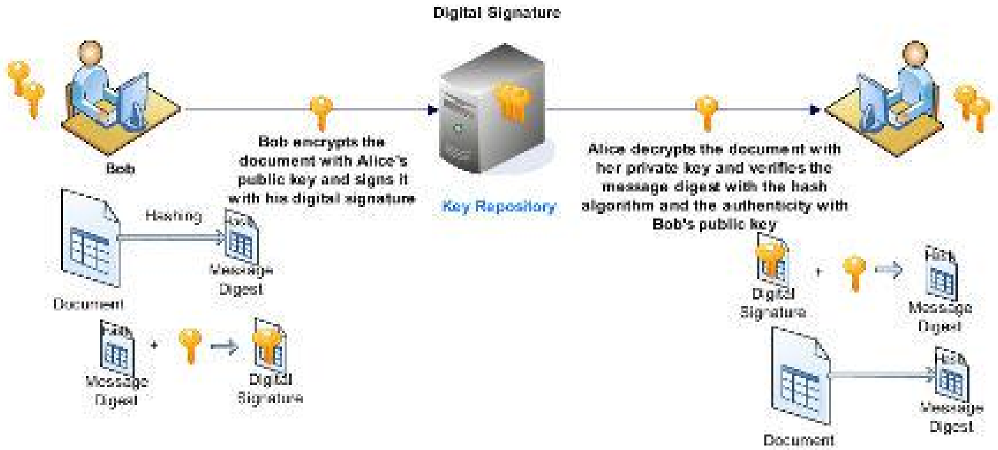

Digital Signature
Bob
Bob encrypts the document with Alice's public key and signs it with his digital signature
Key Repository
Alice decrypts the document with her private key and verifies the message digest with the hash algorithm and the authenticity with Bob's public key
Hashing
Document
Message Digest
+
Digital Signature
Message Digest
Digital Signature
+
Message Digest
Document
Message Digest

Figure 7: MD5 cryptographic Message

Message digest generated from the archives of the above is to 128 bits:

```
0010 1111 1000 0010 1100 0000 1100 1000 1000
0100 0101 0001 0010 0001 1011 0001 1011 1001
0101 0011 1101 0101 0111 1101 0100 1100 0101
1001 0001 1110 0110 0011
```

Then for hexadecimal notation:

```
2F82D0C845121B953D57E4C3C5E91E63
```

3.2 Application Algorithm MD5 for Integrity Data

Application algorithm can be used to maintain to integration data. With the application of the hash function MD5 algorithm into a principle; even small changes in the data can be detected. Steps must be taken is to arouse the contents of a *message digest* of *the* RSIP uses the MD5 algorithm. Then join *the message digest* into the archive. Verify the contents of the archive can be done on a regular basis by comparing the current MD and MD archive contents of the original archive (MD previously saved). If the results are different then there has been a change in the archive.

This application is based on the fact that changes one bit message will change, on average, half the bit-bit *messages digest.* In other words, the MD5 algorithm to hash function is very sensitive to the slightest change in the input data. As an example consider the following records:

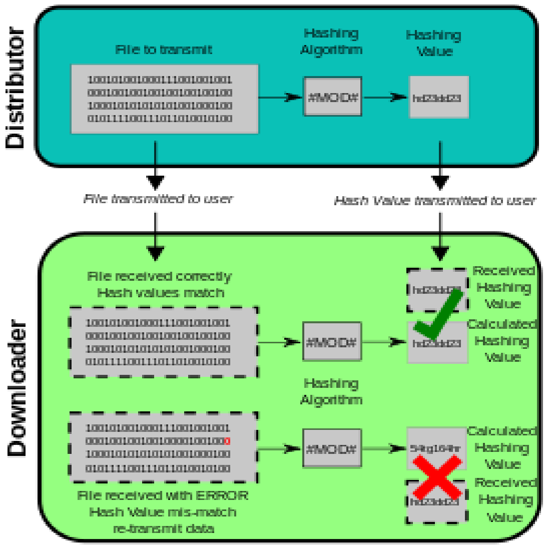


Figure 8: Use of MD5 hashing in file transmission

3.3 System Requirements

The major requirements for the successful implementation and operation of the system are listed below:

- Pentium 4 processor or higher
- 1 GB RAM or higher
- .Net Framework 3.5 or higher
- USB 2.0 port or higher User Operational Manual for the Data integrity checking system guides the user on how he/she will go about using the Software.

3.4 Details

Once the software is launched from desktop The Main/Welcome Screen appears on screen. The Graphical User Interface (GUI) of the main screen has the following:

[1] Checksum Generator Button – when clicked, it enables the user to insert the file(s) that will be hashed

[2] Verification interface Button – On clicking this button, the verification interface is open, where two button are made available for the user, the browse button and verify button. on clicking the browse button, a window is open for the user to choose the desired hash file for comparison. After selecting the hash files, verify button is clicked which execute the comparison and display the result.

[3] Exit Button – This button exit the interface once clicked.

4. CONCLUSION:

Conclusively, the developed system would solve the associated problems with the traditional/manual system. Delay and time consumption will surely be eliminated with the documents being sent over a secure network connection, and an effective & efficient integrity checking system that will guaranty the authenticity of the received document. Similarly, with the successful implementation of this system, confidentiality of messages will definitely be maintained as only authorized personnel of an organization can have access to their systems, unlike the manual system in which junior staffs are charged with the responsibility of delivering mails in the physical sense, so this makes it more prone for the message to be exposed to an outsider who does not have the authority of seen such a confidential message. The prototype of this system has been tasted with different forms of data and it is achieved that the system successfully generates hashes/checksums of a given data, stores them and also performs the verification test and finally give a status report about the message

- Message Digest Algorithm 5 (MD5) algorithm is developed after the algorithm MD2 and MD4.
- *Message Digest* Algorithm 5 (MD5) is a one-way hash function that transforms inputs into outputs with variable length with fixed length is 128 bits.
- With the hash function MD5 algorithm is very sensitive to changes in the message, the MD5 algorithm is suitable for applications that maintain the integrity of the data.

REFERENCE:

1. Arius, Dony., Computer Security, Publisher Andi, Yogyakarta, 2005. https://en.wikipedia.org/wiki/MD5
2. Anigbogu S. O And Inyiama H. C. (2006); Artificial Intelligence-Based Medical Diagnostic Expert System For Malaria And The Related Ailments, Journal Of Computer Science And Its Applications, Vol 12, No 1 P. 3-8.
3. Arjen Lenstra Et Al, (2005) Colliding X.509 Certificates, Cryptology Eprint Archive Report. Http://En.Wikipedia.Org/Wiki/MD5
4. Bert D. B And Antoon B. (1993). Collisions For The Compression Function Of MD5. Available Via: Http://En.Wikipedia.Org/Wiki/MD5 on 11 Aug, 2011.
5. Bellare M. And Rogaway, P. (2005). Introduction To Modern Cryptography. Available Via: Http://En.Wikipedia.Org/Wiki/Cryptography on 14 Sept, 2011.
6. Black F. L. (2003). All About The MD5 Algorithm And How Php Uses It To Encrypt Users' Passwords. Avaiable Via: Http://Www.Neothermic.Com/Kb/Article40.Html on 11 Aug, 2011.
7. Boritz, J. E (2000) "IS Practitioners' Views on Core Concepts of Information Integrity". International Journal Of Accounting Information Systems. Elsevier. Vol 2 No 1.
8. Munir, Rinaldi., Introduction to Cryptography, Bandung Institute of Technology, 2004.
9. Munir, Rinaldi., Hash Function One Direction and MD5 algorithm, Bandung Institute of Technology, 2004.
10. Mulya, Megah., Subjects Cryptography S1, Sriwijaya University, 2008.
11. Thomas, Tom., Network Security First S tep, Publisher Andi 2004.