Authenticity Data through Digital Signature Technique with MD5 Algorithm

Arpan, Nova Mayasari, Muhammad Muttaqin

Abstract*: Data entry must be done by a professional person because this process requires a high level of accuracy. If you enter incorrectly, the results given will also be inaccurate and can even cause misunderstanding. To maintain the authenticity of the data, digital signature techniques are used by using the MD5 algorithm as a hash function that is widely used in cryptographic applications are MD5 and SHA.

Keywords: Digital Signature, Message Digest, MD5.

I. INTRODUCTION

Confidentiality of data in the process of sending data is needed to prevent information from being discovered by unauthorized parties. In addition to the issue of confidentiality, the issue of data authenticity is also very necessary for security, this is because if the recipient receives false data (data that is incompatible with the data sent by the sender) then there will be differences in meaning resulting in chaos and loss on both sides. One technique in using digital signatures is used so that the recipient is guaranteed that the data received is original data not fake data. This technique can prevent the use of false data by the data recipient. Every data received has a signature that is always different from other data, so that a little modification that is done will cause the signature to change very dramatically. [1]

II. REVIEW CRITERIA

a method that directly accesses the records in a table by performing an arithmetic transformation on the key that is the address in the table. The hash function is the most widely used in the security of computer networks and the internet.[2]
MD5 has been used in many fields to secure data authenticity. Broadly speaking, the process of creating a message digest on MD5 includes the following stages: [3]

1. Adding booster bits
   The message is added by a number of bits of the block so that the message length (in bits) is congruent to 448 (mod 512).
2. Adding the original length value
   The message that has been given the booster bits is further added to 64 bits which states the original message length
3. Initialize MD buffer

MESSAGE DIGEST 5
requires 4 buffers with buffer length is 4 32 32 = 128 bits.
can be seen that the buffer will be named A, B, C, and D.
here are initialized with values (in HEX notation) are
A = 01234567
B = 89ABCDEF
C = FEDCBA98
D = 76543210

4. Processing messages on 512-bit blocks

Messages are usually divided into L of 512 bits each (Y0 to YL-1). Each 512-bit block is processed together with the MD buffer into 128-bit output, and this is called the HMD5 process
The process can be seen in the image below: [3]

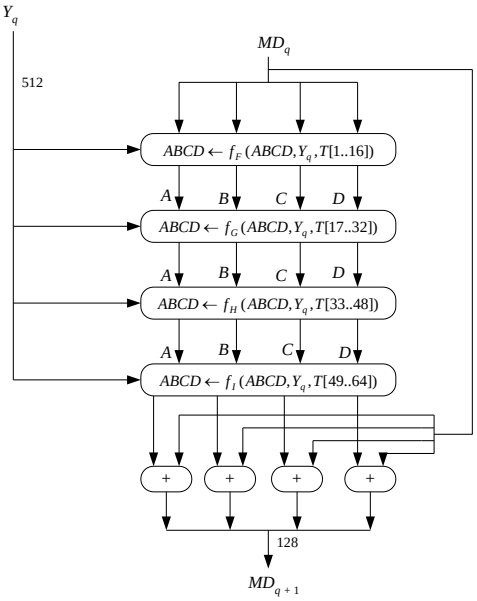


Figure 1. HMD5 process

The HMD5 process consists of 4 rounds, and each round performs MD5 basic operations 16 times and each basic operation uses a T element. So each round uses 16 elements of the T Table.

Revised Manuscript Received on January 5, 2020

Arpan, Lecturer of Computer System Study Program Faculty Of Science And TechnologyUniversitas Pembangunan Panca Budi
Medan City, North Sumatera Provincy, Indonesia

Nova Mayasari, Lecturer of Computer System Study Program Faculty of Science and Technology Universitas Pembangunan Panca Budi
Medan City, North Sumatera Provincy, Indonesia

Muhammad Muttaqin, Lecturer of Computer System Study Program Faculty of Science and Technology Universitas Pembangunan Panca Budi
Medan City, North Sumatera Provincy, Indonesia

III.RESEARCH METHODS

The flow of research in this study is discussed in the diagram below:

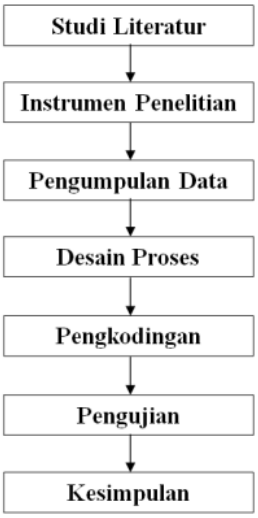
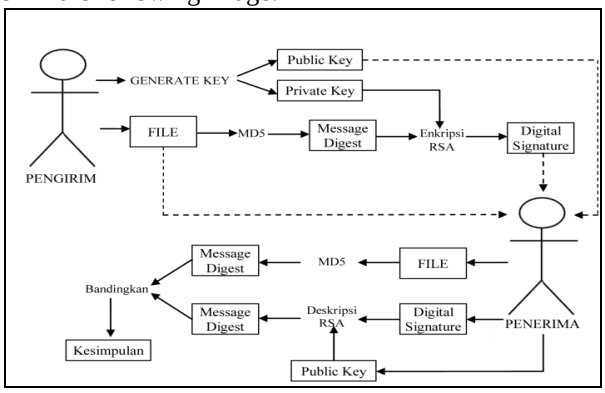


Figure 2. Research Methods

The flow of the digital signature generation process can be seen in the following image:



While the process of testing data authenticity can be seen in the flowchart below:

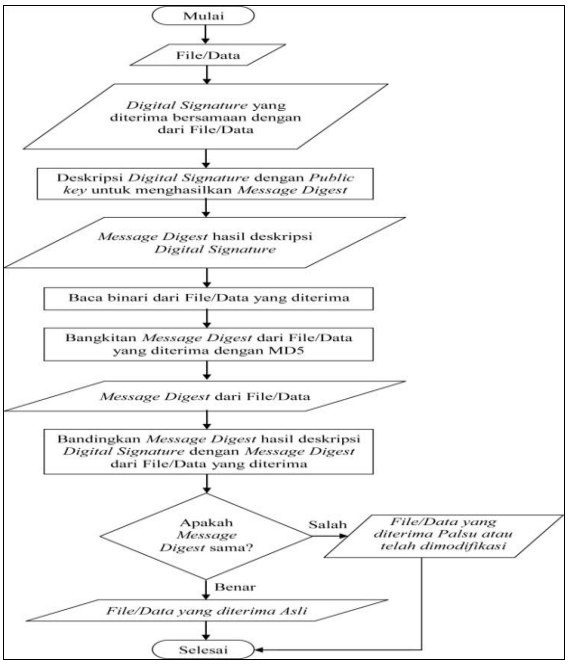


Figure 5. File / Data Authenticity Testing Process

IV.RESULTS AND TESTING

The design process is implemented with the PHP programming language that is run with the Google Chrome browser. The web server that is used is XAMPP 1.7.3.
Testing is done with several types of files. In the first test, an image file was tested, named Apple.jpg.

The program will automatically generate a hexadecimal number form. The resulting digital signature is in the form of a number based on 32. Namely a number consisting of a combination of the following symbols: 0,1,2,3,4,5,6,7,8,9, a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v
Decimal values obtained in digital signatures will be converted automatically by the program into a 32-based number system. The first try can be seen in the following image:

Figure 7. Digital Signature File Generation Results Apple.jpg

File Name: Apple.jpg
Private Key: (849f7, 1d0da7)
Public Key: (7, 1d0da7)
Digital signature: lkdg.18bfi.kq8k.18bfi.kq8k. rno3.18bfi. 1nnc9.40lg.18bfi.18bfi.1nnc9.kq8k.6sil.lkdg.1k8m3.1c5ns .40lg.4fik.kq8k.18fi.sqq.6sil.40lg.0.18bfi.1dmpm.dc7f.1d mpm.1c5ns. Processing time: 0.29151821136475 The Apple. jpg file is sent with the public key, and the digital signature that has been generated. Private key is very confidential and if necessary destroyed, so that no party is able to revive the digital signature through the private key.

Message digest dari Apple.jpg : d2e2e62bc22bead43c8e20aeac029593
PUBLIC KEY : (7, 1d0da7)
Deskripsi : d2e2e62bc22bead43c8e20aeac029593
File belum berubah
Lama Eksekusi : 0.0019059181213379 ms

Digest message from Apple.jpg:
d2e2e62bc22bead43c8e20aeac029593
Public Key: (7, 1d0da7)
Description:
d2e2e62bc22bead43c8e20aeac029593
The file hasn't changed
Processing time:
0.0019059181213379 ms

The results of the second experiment showed that the Apple.jpg file did not undergo modification, so the Apple.jpg file received still maintained its data integrity.

In Figure 8. The results of the second experiment can be seen, the digest message generated from the Apple.jpg file received is: d2e2e62bc22bead43c8e20aeac029593

While the digital signature description results from the original Apple.jpg file give the same results as the message digest from the Apple.jpg file received, which are: d2e2e62bc22bead43c8e20aeac029593. In the third experiment, the Apple.jpg file will be slightly modified with Photoshop by adding a very small blue dot.

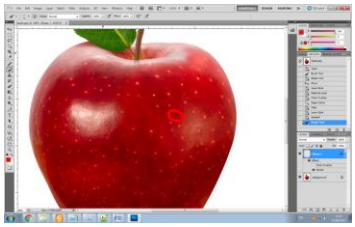


Figure 9. Modifications to the apple.jpg file

After the apple.jpg file has been modified, a fourth experiment will be performed to find out if a slight modification of the file will cancel the digital signature. The fourth experiment can be seen in the following picture:

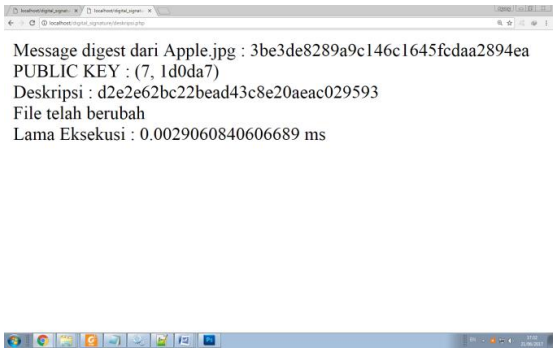


Figure 10. Fourth Experiment Results

The fourth trial result shows that the file has changed, the digital signature or the given digital signature has been canceled by the received Apple. jpg file, so the Apple.jpg file that has been received has been modified so that the data integrity of the Apple.jpg file has been attacked.

In Figure 9, the results of the fourth experiment can be seen, the digest message generated from the Apple.jpg file received is: 3be3de8289a9c146c1645fcdaa2894ea

While the digital signature description results from the original Apple.jpg file are: d2e2e62bc22bead43c8e20aeac029593

Table 1. Results of experiments on several file formats

No	Format File	Size dan Key	Key	*Digital signature*	processing time
1	.docx	78.9 KB	*private key*: (ab007, 257483) *public key*: (7, 257483)	74ds.1h19m.9bfp.2aj23.1i711.1apct.s4g4.1.1r76v.s2bc.74ds.s4g4.2aj23.28pj5.28pj5.0.mi54.74ds.28pj5.28pj5.1h19m.28pj5.1ovdl.1ovdl.1apct.1ovdl.1i711.28pj5.28pj5.74ds.1r76v.1h19m	0.604543924 33167
2	.xlsx	34.9 KB	*private key*: (1a9123, 1d442d) *public key*: (b, 1d442d)	0.1m39l.1jek1.vcda.e8lt.9h6f.1hcrc.1jek1.1hcrc.1.17kg7.1jek1.1hcrc.d7ob.722v.vcda.1.1qaau.1m39l.17kg7.e8lt.722v.9h6f.hv2q.hv2q.1gce6.e8lt.0.vcda.vcda.1hcrc.e8lt	1.221235990 5243
3	.txt	9.03 KB	*private key*: (5530d, 1aa997) *public key*: (5, 1aa997)	p2si.14r7t.0.lrh6.ge99.42ka.0.42ka.1cts9.0.1a6k1.14r7t.ge99.14s9p.1cadj.1cts9.p2si.42ka.h2gf.1a6k1.5do.5do.lrh6.h2gf.5do.1cts9.0.1cadj.14s9p.1cadj.1.5do	0.199546098 70911
4	.rar	2.68 MB	*private key*: (167aa1, 258355) *public key*: (5, 258355)	1hku7.1hku7.10pi1.16cet.21ui8.qmi3.t09q.79fu.1fch4.qmi3.21ui8.16cet.sqkf.1fch4.1gn77.1h98b.1qdbe.t09q.1gn77.qmi3.qmi3.1hku7.1qdbe.qmi3.21ui8.79fu.1gn77.1.79fu.dpnv.sqkf.21ui8	1.343211174 0112
5	.mp3	4.15 MB	*private key*: (1d88ad, 314735) *public key*: (5, 314735)	1mm15.of0.1mmpu.sk4.1mmpu.10bdg.10bdg.84up.1vfmu.1qlnc.2mg22.2mg22.lpll.1qlnc.1qlnc.2dujb.0.41qq.1vfmu.0.sk4.1vfmu.1qlnc.1mmpu.1mmpu.1qlnc.lpll.1vfmu.10bdg.84up.lpll.84up	1.751899003 9825
6	.pdf	132 KB	*private key*: (173737, 1b2081) *public key*: (7, 1b2081)	b120.1.9553.1.irtp.1.g7n7.2rqc.0.1lo6s.9553.0.0.2rqc.2fih.apr5.apr5.0.2rqc.g7n7.71ol.15018.71ol.apr5.irtp.b120.9553.2fih.apr5.13h63.irtp.g7n7	0.842025041 5802
7	.mp4	3.54 MB	*private key*: (d5e1b, 14161f) *public key*: (3, 14161f)	thd7.heb2.2ssq.2ssq.13562.2.2ssq.1.10pus.10d0u.0.2.mcg3.heb2.1.2.81hd.10pus.81hd.13562.thd7.8qu9.10d0u.1.du5f.1.2ssq.9uug.2ssq.du5f.1.9uug	0.594333887 10022

V. SECURITY ANALYSIS

Without a private key, it cannot be just anyone who can generate a digital signature from a data. If the attacker uses any private key, then the public key pair used by the recipient of the data will not match. Because different private keys will provide different public

key pairs. Therefore, to strengthen the digital signature scheme, the private key should only be used for one time and immediately destroyed if it has been used to generate a digital signature so that it can no longer be used by other parties. MD5 processes variable length messages through input messages that are broken up into sections with sixteen endian blocks of thirty two message bits so that their length is divided by 512. This padding is between the main content and the broder which has a function like the first single bit added at the end of a sentence. This is followed by as many zeros as is needed to bring the message length to 64 bits less than a multiple of five hundred and twelve. The remaining bits are filled with sixty four integers representing the length of the original message in the bits. The main MD5 algorithm operates in conditions of one hundred twenty-eight bits symbolized A, B, C or D. This main algorithm operates on each block of messages as many as 512 bits in turn, each block modifying its portion.

VI. CONCLUSION

From the experiments that have been done, digital signatures can provide security against the authenticity of the data, so that the recipient avoids using fake data that has been modified by the attacker to the detriment of the recipient or sender of the file. The slightest change that occurs to the data, will significantly change the existing digital signature, so that it will automatically cancel the digital signature given previously to the file.

Digital signatures can be generated by a combination of MD5 and RSA algorithms. The combination of these two algorithms can provide increased security for data authenticity. The MD5 algorithm has a 128-bit output, so it has 2128 possible combinations. The RSA algorithm prevents so that not just anyone can generate a digital signature from existing data, only the sender who has a private key can generate a digital signature. So the combination of these two algorithms will provide a high level of security.

REFERENCES

1. Noroozi, N., Daud, S. M., Sabouhi, A. (2013). Secure *Digital Signature* Schemes Based on Hash Functions. International Journal of Innovative Technology and Exploring Engineering (IJITEE) Volume-2, Issue-4
2. Jacob, N. M. (2015). Vulnerability of data security using MD5 function in php database design. EPH International Journal of Science and Engineering, 1(1), 11–15.
3. Walia, P., & Thapar, V. (2014). Implementation of new modified MD5-512 bit algorithm for cryptography. International Journal of Innovative Research in Advanced Engineering (IJIRAE), 1(6), 2349–2163.
4. Kallam, R. B. (2011. An Enhanced RSA *Public key* Cryptographic Algorithm. International Journal of Advanced Research in Computer Science (IJARCS)
5. Singh, S. (2013). A Performance Analysis of DES and RSA Cryptography. International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
6. Schneider, M.-. A Robust Content Based Digital Signature For Image Authentication. Columbia University
7. Singh, S. (2015). Survey on Techniques Developed using Digital Signature: Public key Cryptography. International Journal of Computer Applications
8. Krishna, D. S. R., (2015). Providing Security to Confidential Information Using Digital signature. International Journal of Advance Research in Computer Science and Management Studies
9. Shankar, M. (2014). Hybrid Cryptographic Technique Using RSA Algorithm And Scheduling Concepts. International Journal of Network Security & Its Applications (IJNSA) 6(6), 39–48.
10. R. Munir,. 2006. Kriptografi. Bandung; Informatika.

AUTHORS PROFILE

Arpan, Strata 1 University Of Panca Budi Development University Medan Computer Systems Study Program. Strata 2 University Of Amikom Jogyakarta Informatics Engineering Study Program. Publications With The Title: 1) Base 64 Character Encoding And Decoding Modeling, 2) Analysis Of Knowledge Management Sharing Implementation On Web-Based Academic Portals In The Era Of Panology In The Era Of Digital 4.0 Technology 4.0 In The Era Of Digital Now. Researcher Work: 1) Information Technology Consultant, 2) Structural Staff At Panca Budi University Development 3) Lecturer In The Faculty Of Science And Technology UNPAB (Computer System Study Program)

Nova Mayasari, Strata 1 University of Panca Budi Development University Medan Computer Systems study program. Strata 2 University of Amikom Jogyakarta Computer Science study program. Publication titles: 1) Comparison Of Support Vector Machines and Decision Trees in Predicting On-Time Graduation, 2) Vehicle Plate Recognition Using Template Matching, 3) Data Mining Implementation to Predict Sales Promotion Itemset on CV. Main Fresh Source. Research Work: Lecturer in the Faculty of Science and Technology UNPAB (Computer Systems Study Program)

Muhammad Muttaqin, Strata 1 University of Panca Budi Development University Medan Computer Systems study program. Strata 2 University of Amikom Jogyakarta Informatics Engineering study program Publication of title: 1) A Review of IP and MAC Address Filtering in Wireless Network Security, 2) Analysis Of Use Of E-Office Information Systems In The Medan Development University Of Panca Budi Medan Using The Utaut Method. Research Workers: 1) IT Consultants, 2) Structural Staff at Panca Budi University Development, 3) Lecturers of the Faculty of Social Sciences UNPAB (Computer System Study Program), 4) Soft Skill Training Trainers at Abdi Training