International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 04 Issue: 06 | June -2020 ISSN: 2582-3930

A Study on Integrity and Authentication Algorithms in Data Security

P.M.Pazhani Selvam M.C.A. ,M.Phil[1]., Dr.S.S.Sujatha, M.C.A.,M.Phil.,Ph.D[2]

[1]Research Scholar(Reg. No: 18123152161002), ManonmaniamSundaranarUniversity,Tirunelveli-627012.
[2]Associate Professor, Department of M.C.A., S.THindu College, Nagercoil-629001.

Abstract: In data communication, security is implemented using privacy, authenticity, integrity and non-repudiation concepts. Privacy is maintained using symmetric encryption algorithms. Authentication is implemented using the algorithms which create digital signatures. Integrity is kept up with integrity algorithms which create message digest, hash value, etc. Non-repudiation is implemented with the help of trusted third parties, who are ready to sign on the digital signatures. This paper analyzes the various message integrity and message authentication algorithms.

Key words: Authentication, Integrity, Message digest, Digital Signature,Hash algorithms.

1.INTRODUCTION

Message integrityensuresthat the data arenot modified **d**uring the data communication and message authentication ensures that the data are received from an authentic person. Authentication is a process which needskey generation algorithm, signing algorithm and verifying algorithm[1].Message authentication is done with the help of Message Authentication Code (MAC) and message integrity is done with the help of Message Detection Code (MDC).

1.1.Message Integrity

Message digest algorithms are used to ensure data integrity. Hashing algorithms are nothing but the message digest algorithms. Sender combines a secret key, with the data and calculate the hash value and include it with the sending data. With the same secret key, the receiver again calculates the hash value of the received data and compare it with the hash that is already sent. If there is no difference, the receiver confirms that the data is not modified.The hashing algorithm ensures that the data is not modified [2].

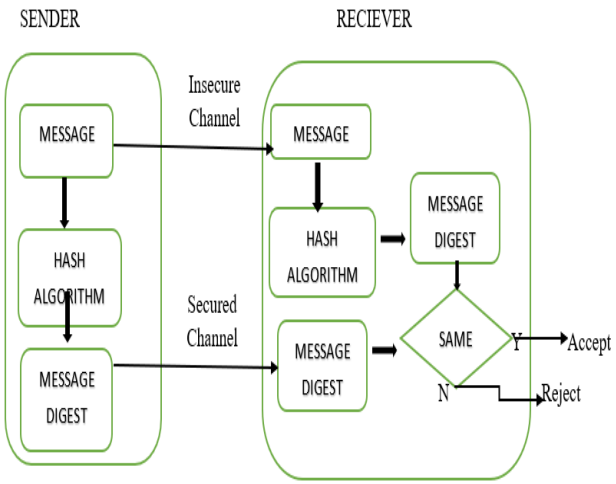

Fig 1.1.1 Message Integrity

1.2.Message Authentication

Message authentication uses asymmetric keys. The digital signature algorithm of the sender calculates the MAC(Message Authentication Code) using the secret data and private key of-- the sender. The secret data and MAC are received by the receiver and receiver verifies the MAC using the secret data and public key of the sender. If the receiver receive the same MAC, then the receiver accept the data, otherwise the data is rejected [5]. Sometimes the digital signature algorithm is applied more than one time in both sides. This process is called nested message authentication.

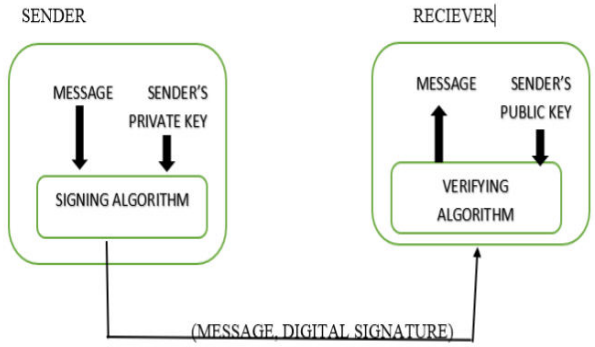

Fig.1.2.1 Message Authentication

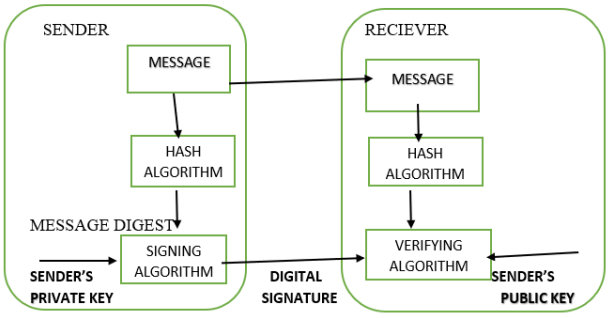

Fig. 1.2.2 Signing the Digest

1.3.Digital Signature

It is nothing but Message Authentication Code (MAC). Every data file corresponds to one digital signature. Sender signs the sending data using sender's private key. Sender uses signing algorithm for to create digital signature. The created digital signature and data are sent to the receiver. The receiver verifies the authenticity of both data and signature using sender's public key. The receiver uses verification algorithm for the verification of digital signature. If the result is true, accept the data, otherwise rejected [5]. Suppose, if the data is modified, it is not possible to get the same digital signature. It is possible to generate digital signature for message digest.Thus a digital signature maintain authenticity as well as integrity.

1.4.Message Digest

It is used to test message integrity. Using hash algorithms, from the secret data, message digest is created. It is also known as hash value. The message digest is in fixed length.For every message, one corresponding message digest created. There are no common message digest for two messages(data). It is also possible to generate digital signature for message digest. Thus authentication is also applied with message integrity [5].

2.HASH ALGORITHMS

The Hash algorithm is a one-way-function and used to ensure the data integrity.It convertsan arbitrary-length data to a fixed-length output.The hashing algorithm calculates message digest. The message digest should be protected from changes. Data(message) and message digest are sent to the receiver. The receiver again calculates the message digest of the received data and compares it with the message digest that is already sent. If there is no difference, the receiver confirms that the data is not modified.The digest created by the hash function is called Modification Detection Code (MDC) [5].CRC algorithm is thefirst initiator of data integrity work. It uses associativity concept [6]. The next initiator is MD2. In 1989, Ronald L. Rivest designed MD2, a hashing algorithm. Then it is revised and MD4 is published in 1990. MD5 is a hashing algorithm, which accept a message of size 2^{64}-1 bits and reduce it as a digest of 128 bits. MD5 is the popular algorithm and preferred by many people.MD6 is another one hashing algorithm developed in 1993. It has four variations. They are MD6-224,MD6-256, MD6-384 and MD6-512.

Table 2.1.Characteristics of Hash Algorithms[8]

	MD2	MD4	MD5	MD6-224	MD6-256	MD6-384	MD6-512
MMS	2^{64}-1	2^{64}-1	2^{64}-1	2^{64}-1	2^{64}-1	2^{64}-1	2^{64}-1
BS	512	512	512	512	512	512	512
MDS	128	128	128	224	256	384	512
NR	18	3	5	96	104	121	168
WS	64	64	64	64	64	64	64

MMS:Maximum Message Size(bits)
BS: Block Size(bits)
MDS: Message Digest Size(bits)
NR: Number of Rounds(numbers)

WS: Word Size(bits)

2.2.Merits

Man-in-the-middle attack is easily detected by hashing algorithms [5].

2.3.Limitations

MD algorithmsare failure to face collision attacks. MD4 is faster than MD5.MD5 algorithm is slower compared to secured hash algorithms [3].

3.SECURED HASH ALGORITHMS (SHA)

They are used in a wide range. These algorithms are developed by National Institute of Standards and Technology(NIST) and published as a United States Federal Information Processing Standards(FIPS). There are four different variations of SHA. They are SHA-0(1993),SHA-1(1993),SHA-2(2001) and SHA-3(2012). The first two support 160 bits hash function.SHA-1 works like MD5 algorithm. SHA-2 has four different variations. They are SHA-224(32 bits word),SHA-256(32 bits word), SHA-384(64 bits word) and SHA-512(64 bits word). NIST added Keccak algorithm with SHA-3. It's length is similar to the previous version SHA-2, but the internal structure is different[7]. It is speedy and takesminimum number of rounds than others. It is one of the Standard Hash Algorithm [6].

Table 3.1.Characteristics of Secured Hash Algorithms

	SHA-0	SHA-1	SHA-224	SHA-256	SHA-384	SHA-512	SHA-3
MMS	2^{64}-1	2^{64}-1	2^{64}-1	2^{64}-1	2^{128}-1	2^{128}-1	2^{128}-1
BS	512	512	512	512	1024	1024	1024
MDS	160	160	224	256	384	512	512
NR	80	80	64	64	80	80	24
WS	32	32	32	32	64	64	64

MMS:Maximum Message Size(bits)
BS: Block Size(bits)
MDS: Message Digest Size(bits)
NR: Number of Rounds(numbers)
WS: Word Size(bits)

3.1.Merits

Generally secure hash algorithms provide high security than hashing algorithms [5]. They easily handled man-in-the-middle attacks.

4.DIGITAL SIGNATURE ALGORITHMS

4.1.RSA Algorithm

It is an asymmetric key algorithm, which is used to implement authentication by generating digital signature. The basic principle behind authentication is only the authentic person, who holds the secret private key can decrypt the message. RSA is slow, because the keys are very large. So, it is desirable to use RSA to generate digital signature and to protect the symmetric keys used to encrypt and decrypt the secret data [7]. RSA cryptosystem uses the private and public key of receiver. But RSA digital signature uses of the private and public key of sender [5].In RSA algorithm, using sender's private key, the digital signature is made and using sender's public key the digital signature is verified. It creates digital signature from the secret data itself.

4.1.1.Limitations

RSA consumes more time to generate digital signature for a lengthy message. The alternative approach to be followed is to sign on the digest, whichis created by hashing algorithms. This approach takes less time to generate digital signature. At the same time, it implements integrity.

4.2. ECDSA(Elliptic Curve Digital Signature Algorithm)

This algorithm was developed by Neal Kobilitz and Victor Miller, which was accepted by ANSI in 1999 and also accepted by IEEE and NIST standards in 2000. It also has three important operations. They are key generation procedure, which generates private and public key pairs. Other two are signing and verification operations. It is also an important message authentication algorithm, which creates digital signature [9].

4.2.1.Merits

The algorithm needs less memory and less time to finish the work. It implements greater security with

small key sizes. It requires small hardware chips and less power consumption.

4.2.2.Limitations

This algorithm is very slow in encryption and verification work. Some update algorithms like Montgomery, needed to improve its speed.

4.3.Digital Signature Algorithm

In1991,National Institute Standards and Technology(NIST) announced DSAas a Digital Signature Standard and adopted it as Federal Information Processing Standard(FIPS 186) in 1994. Then four variations have arrived. It is used to create digital signatures. It has four important operations. They are key generation, key distribution, signing and signature verification. Key distribution means sender sends the keys to receiver. This algorithm generates a digital signature which consists two 160-bits numbers. It is also one of the digital signature algorithm widely preferred [4].

4.3.1.Merits

This algorithm takes less time and storage area to generate digital signature. This is also free of cost. The key pairs sizes are very small compared to RSA.

4.3.2.Limitations

This algorithm depends on hashing algorithms. It generates digital signature from only on message digest.

Table 4.1. Characteristics of Digital signature algorithms

	RSA	ECDSA	DSA
Key size (bits)	Large(1024, 2048,4096)	Small(192,256)	Small(320)
Block size	Small	Large	Large
Encrypted message size	Large	Small	Small
Computational power need	More	Less	Less
Speed	Slow	Fast	Fast
Storage space need	More	Less	Less
Signing speed	Slow	Fast	Fast
Verification speed	Fast	Slow	Slow
Encryption speed	Fast	Slow	Slow
Decryption speed	Slow	Fast	Fast
Domain	Heavy weight devices like Computers , Laptops.	Light weight devices like Tablets, Smart phones.	Light weight devices like Tablets, Smart phones.
Technology	Integration of Factors	Discrete logarithm	Discrete logarithm
Authentication	Very high	High	High

5.RESULTS AND DISCUSSION

5.1. Comparison of cryptographic algorithms

Table 5.1. Comparison of Cryptographic Algorithms

Security Factors	Digital Signature Algorithms	Secure Hashing Algorithms	Hashing Algorithms
Privacy	No	No	No
Authentication	Yes	No	No
Integrity	Yes	Yes	Yes
Non-Repudiation	Yes	No	No

Message Digest (Hashing) algorithms are often affected by collision attacks. Their performance is lower than Secure Hash Algorithms. Compared to hashing algorithms, Secured Hash Algorithms provide fast execution and better security. But these two categories of algorithms are used to test data integrity. The digital signature algorithms are used to test data authentication. They are also used to sign the message digest produced by hashing function. If any changes in the message digest, then it is not possible to produce the same signature. Thus digital signature algorithms provide data integrity also. If the third parties are willing to sign a data file, using digital signature algorithms, then non-repudiation work is also possible.

5.2. Comparison of Digital Signature Algorithms

To compare the digital signature algorithms, the following three factors are considered.

1. The time taken to generate key pairs
2. The time taken to sign the message
3. The time taken to verify the signature

Table 5.2.1. Time taken by RSA algorithms (in seconds)

Key length (bits)	RSA-512	RSA-1024	RSA-2048	RSA-4096
Key generation	0.132	0.431	2.559	112.3
Signing	0.00009	0.000315	0.001805	0.010827
Verification	0.000007	0.000019	0.000062	0.000194

Table 5.2.2. Time taken by ECDSA algorithms (in seconds)

Key length(bits)	ECDSA-160	ECDSA-192	ECDSA-224	ECDSA-265	ECDSA-384	ECDSA-526
Key generation	0.165	0.181	0.242	0.315	0.822	1.765
Signing	0.00035	0.00037	0.00074	0.00092	0.002	0.0043
Verification	0.0017	0.002	0.003	0.005	0.0092	0.02

A 192 bits ECDSA algorithm performs equal to 1024 bits RSA algorithm. A 256 bits ECDSA algorithm performs equal to 2048 bits RSA algorithm [9].

Table 5.2.3. Time taken by DSA algorithms (in seconds)

Key length (bits)	DSA-160	DSA-224	DSA-256
Key generation	0.178	0.274	0.295
Signing	0.0004	0.0008	0.0012
Verification	0.0013	0.0032	0.004

A 160 bits DSA algorithm performsequal to 1024 bits RSA algorithm. A 224 bits DSA algorithm performs equal to 2048 bits RSA algorithm. A 256 bits DSA algorithm performs equal to 3072 bits RSA algorithm [10].

5.3. Charts

Key generation process takes more time than signing process and verification process.

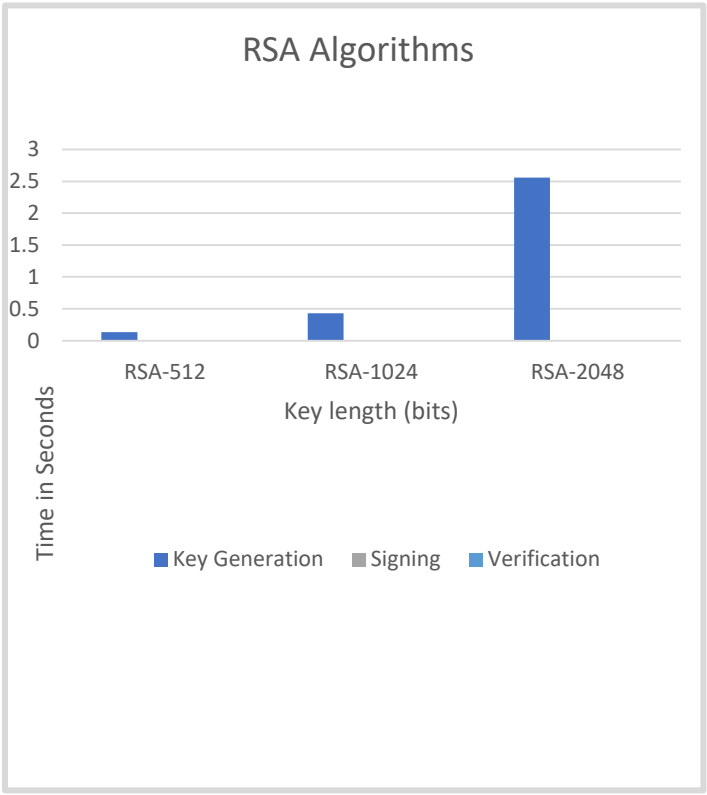

Fig 5.3.1. Time taken by RSA algorithms for key generation, Signing and Verification

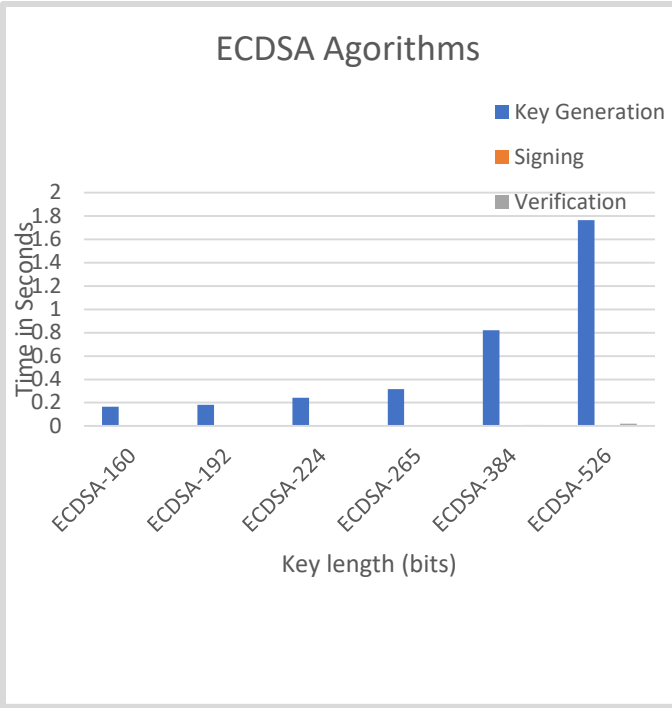

Fig 5.3.2. Time taken by ECDSA algorithms for key generation, Signing and Verification

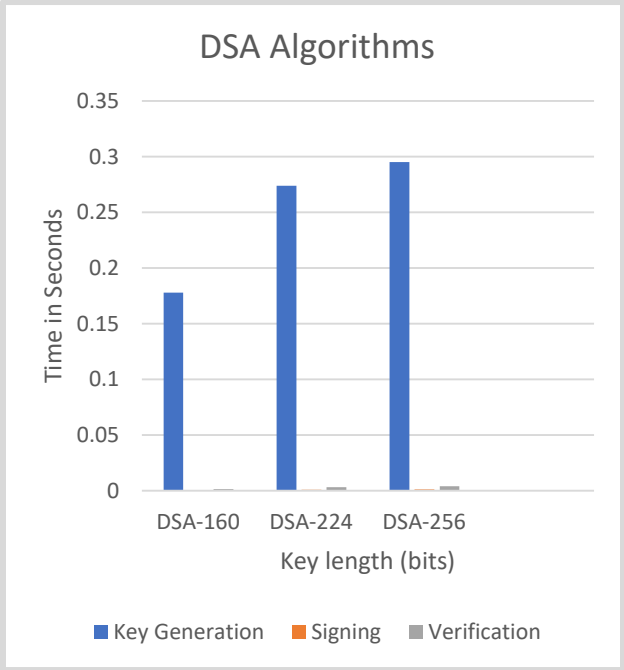

Fig 5.3.3. Time taken by DSA algorithms for key generation, Signing and Verification

RSA consumes more amount of time to generate keys than other two algorithms

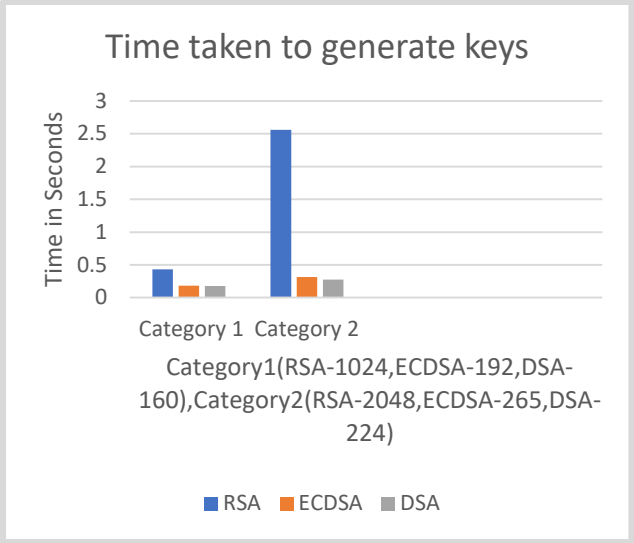

Fig 5.3.4. Time taken by different algorithms for generating keys.

RSA takes less time than other two algorithms, when the key size is small. RSA takes more time than other two algorithms, when the key size is large.

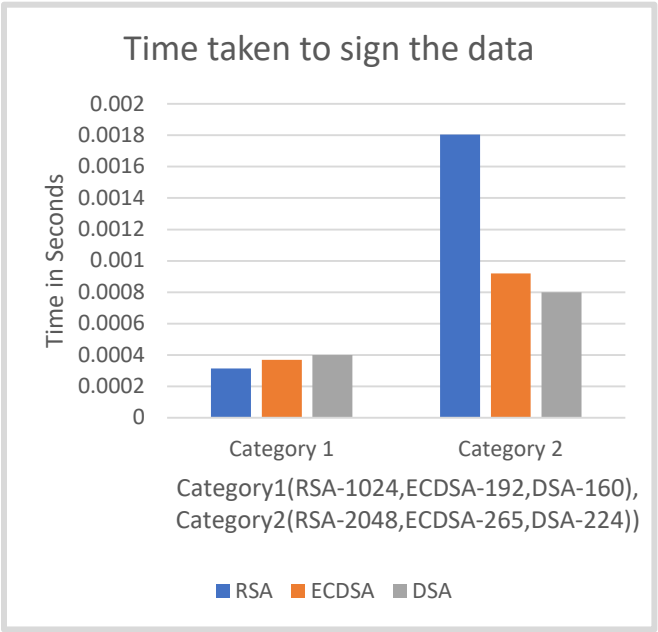

Fig 5.3.5. Time taken by different algorithms for signing data

RSA consumes less time than other two algorithms in the verifying signature process

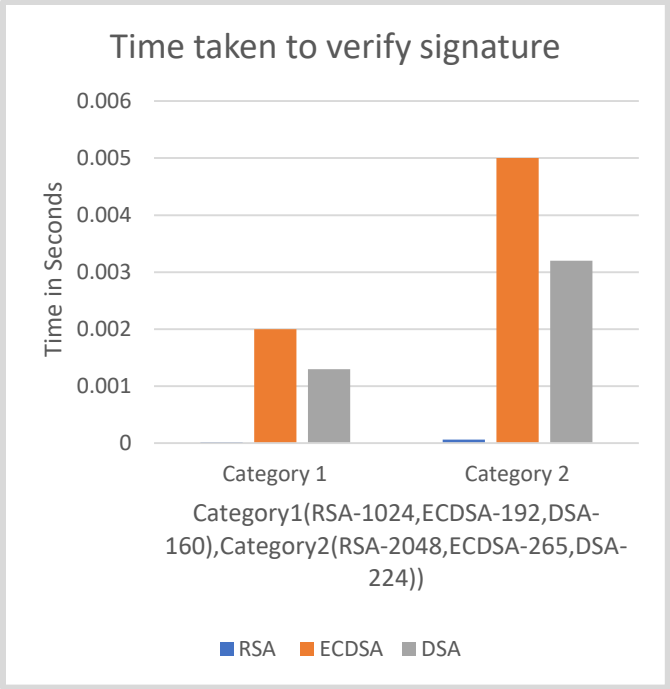

Fig 5.3.5. Time taken by different algorithms for verifying Signature

RSA performs well when key sizes are small. Other two algorithms are very slow in the process of decryption and verification. RSA gives more security than other two algorithms. RSA is suitable for the devices like Personal Computers and Lap Tops. The other two algorithms are suitable for light weight devices.

6.CONCLUSION

In this paper, various hashing algorithms, secure hashing algorithms and digital signature algorithms are analyzed to implement message integrity and message authentication in a secured communication. Secured hash algorithms are faster and provide more security than hashing algorithms. But these two categories of algorithms are suitable for testing data integrity only. But they are not supporting data authentication work. The digital signature algorithms are suited to test data integrity and data authentication. Within digital signature algorithms, RSA performs better than other algorithms. DSA depends on any hashing algorithm to create digital signature. ECDSA and DSA shows their weakness in verification and decryption process. RSA is a cryptographic algorithm which is used to encrypt/decrypt data, exchanges secret keys, ensures integrity and authentication and also supports non-repudiation process. RSA algorithm is more suited to test integrity and authentication in a secured communication.

REFERENCES

1.“https://en.wikipedia.org/wiki/Message_authentication_code”
2.Message Integrity”, 18th September 2015, “https://www.practicalnetworking.net/series/cryptography/message-integrity”.
3. “Message-Digest Algorithm 5 (MD5) in Cryptography”, Monika Sharma, on January 09, 2020,“https://www.includehelp.com/cryptography/message-digest-algorithm-5-md5.aspx”.
4. ”Digital Signature Algorithm”,From Wikipedia, the free encyclopedia, “https://en.wikipedia.org/wiki/Digital_Signature_Algorithm#Key_distribution”.
5. Behrouz A. Forouzan, “Cryptography and Network Security”, First Edition, Tata-McGraw-Hill Publishing Company Limited, New Delhi.
6.Paul Svasta, Andrei Marghescu, TraianNeacsa ,“Cryptographic Coprocessor for Data Integrity Algorithms”, 37th Int. Spring Seminar on Electronics Technology, 978-1-4799-4455-2/14/$31.00 ©2014 IEEE.
7.K.Devika, M.Jawahar, “Review On: Cryptographic Algorithms for Data Integrity Proofs in Cloud Storage”.International Journal of Engineering Trends and Applications (IJETA) – Volume 2 Issue 1, Jan-Feb 2015.
8. Md. Alam Hossain, Md. Kamrul Islam, Subrata Kumar Das and Md. Asif Nashiry, “CRYPTANALYZING OF MESSAGE DIGEST ALGORITHMS MD4 AND MD5”, International Journal on Cryptography and Information Security(IJCIS),Vol.2, No.1,March 2012.
9. Al Imem Ali, “COMPARISON AND EVALUATION OF DIGITAL SIGNATURE SCHEMES EMPLOYED IN NDN NETWORK”, International Journal of Embedded systems and Applications(IJESA) Vol.5, No.2, June 2015.
10.K.Sivaraman, “A COMPARISION STUDY OF RSA AND DSA ALGORITHM IN MOBILE CLOUD COMPUTING”, International Journal of Pure and Applied Mathematics, Volume 116 No. 8 2017, 247-253.