International Journal of Pure and Applied Mathematics
Volume 116 No. 8 2017, 247-253
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue

ijpam.eu

A COMPARISION STUDY OF RSA AND DSA ALGORITHM IN MOBILE CLOUD COMPUTING

K.Sivaraman
Assistant Professor, Dept. of CSE, Bharath Uni versity,
Chennai, Tamil Nadu, India,
sivaraman2006@gmail.com

Abstract: In Mobile Cloud computing set of information that are shared with multitenant users. So many security and privacy issues may arise. In cloud computing we can store data and information regarding sender and receiver on cloud through mobile applications. In this mobile cloud computing the devices are not having enough space to store and secure all information. So, the paper is to study the comparison of two methods RSA (Ronald Rivest Algorithm) and DSA (Digital Signature Algorithm to assure privacy and security of data cryptographic.

Keywords: Mobile cloud computing, security, privacy, information, encryption, data cryptographic.

1. Introduction

Mobile Cloud Computing has provided an enormous online storage for mobile users, but the most serious issue faced by the users is to trust the third parties, that is, the cloud vendors and their partners[1,5,6]. Mobile Cloud computing is an amalgamation of three important parts. They are cloud computing, mobile internet and mobile devices. The significant of security and privacy protection deals mainly with social networks, cloud computing and mobile computing. At present, the most frequent issue arising for mobile users in mobile computing or any other business is security and privacy protection. Encryption is considered as the most secured method in cloud computing[2,3]. Encryption is referred to as a method of secure communication which prevents the accessing of data by third-parties while interchanging data between two devices[4].

It is not possible to use encryption. In mobile devices. So, this paper is about the study of RSA and DSA algorithm for privacy and security of data cryptographic. In RSA algorithm The properties of the Multiplicative Homomorphic encryption is realized by RSA cryptosystem. The RSA algorithm was invented by Ronald Rivest, Adi Sharmir, and Leonard Adleman. and they named after its inventors. Theexponential modular is used for decryption and encryption in RSA. In RSA algorithm two elements are used as a and b where a is public key and b is private key[7,8]. In DSA algorithm, the public key primitives of message authentication by digital signature. They are utilized to tie signatory to the message. The cryptography value is calculated from the secret key and private data only known by the singer of digital signature.

2. DSA Algorithm

The DSA generally refers to the Digital Signature Algorithm. The RSA however refers to the initials of the people who created it. These are Ron Rivest, Adi Shamir, and Leonard Adlemanm , The DSA become designed as an encryption algorithm. The DSA was advanced by the NSA to be utilized by the United States government as a standard for virtual signatures. This signature borrows closely from the ElGamal Signature Algorithm from which maximum thoughts had been borrowed from. RSA, on the other hand[9,10], seems at the issue of factoring numbers as the primary issue of its improvement.

The name DSA spells out its dominant characteristic. This is a software that is especially constructed for signing, and consequently it is pretty famous with virtual signatures. This however does now not extend beyond the signature to the message itself. RSA, on the other side, covers signing in encryption and encryption of the message contained as well.

As a result of managing virtual signatures best, the use of DSA is preferred while faster key technology is wanted. This is due to the fact DSA produces the keys right away. When faster encryption is needed, RSA is favored because it encrypts each message and signature for signing in. When in need of decryption, DSA is faster particularly because of the truth that it's miles specialised for a single function simplest. Digital signature technology work fine with DSA while verification of the virtual signature is quicker while RSA is hired. In looking at how quick both DSA or RSA handles a given venture, it need to be assessed whether or not fewer computer resources are used.

A perfect stability should be found which employs both DSA and RSA, as no unmarried encryption set of rules may be rolled out on my own. Both the RSA and DSA are essential in rolling out encryption algorithms that may be employed within the server surroundings and with the patron as nicely.

Both the RSA and DSA can be stated to have similar cryptographic strengths. It is but the overall performance blessings whilst rolling out at specific factors that make one or the opposite the desired preference to be used at that unique point in time [11,12,13].

It may be generally concluded that the DSA is first-class ideal for signing in and decrypting even as verification and encryption can be left to the RSA. If any issue is stated with the overall performance, an assessment can be performed to find out if the proper encryption algorithm has been rolled out.

RSA Algorithm:

An RSA crypto-set of rules ("encryption key") ("decryption key") is based on large-variety factorization. i.e., P * Q = N, with a couple of different beneficial suggestions (you cannot just select any P or Q), and it takes numerous computers a totally long time to break N returned up into its unknown P * Q elements.

Cryptographic:

A DSA crypto-algorithm ("encryption key") ("decryption key") is primarily based on discrete logarithms -- i.E., B to the K energy = G, with multiple other useful hints (you cannot simply pick any B or K), and it takes a number of computer systems a totally long term to get better that K exponent which makes the equation paintings.

There isn't any clean 'winner' between the 2 methods. DSA is a chunk quicker than RSA when developing a signature (an encrypted token to be used by one or both facets), however slower than RSA while analyzing/validating that signature (token). Similarly, DSA is faster to decrypt, but slow(er) to encrypt; RSA is contrary[14,15].

There is a few "hassle" in using extra-than-1024-bit DSA in FIPS compliant cryptography; I don't fully apprehend it, however RSA does not showcase the hassle, and hence 2048-bit RSA is not unusual, in assessment to 1024-bit DSA. Speaking only for myself, I type of appreciate DSA's relative strengths.

It is faster to decrypt -- and genuinely, over the life of a cryptosystem, we will decrypt messages more than we will encrypt them (esp. If the message has a couple of recipients).

Additionally, the DSA algorithm just plain doesn't have as a lot interest focused on it. Some will argue that is simply 'security thru obscurity,' however I contend that, whilst one set of rules is 'damaged,' it'll be RSA large-wide variety factorization that topples first. Bottom line: each are 'sufficiently sturdy,' and feature most effective minor differences[16,17,18].

Use whichever works for you, satisfies your 1024-or-2048-or-something alternatives, and is supported by way of your UNIX/Windows/other utility.

Digital signature model

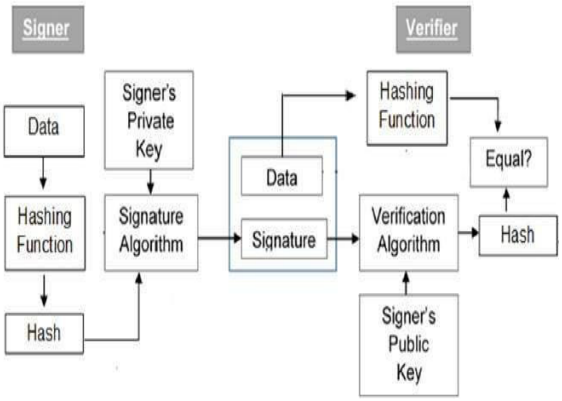

Figure 1. Model of Digital Signature

The accompanying focuses clarify the whole procedure in detail –

- Each individual receiving this plan has an open private key match.
- Generally, the key sets utilized for encryption/decoding and marking/confirming are distinctive. The private key utilized for marking is alluded to as the mark key and people in general key as the check key[19,20].
- Signer sustains information to the hash work and creates hash of information.
- Hash esteem and mark key are then nourished to the mark calculation which delivers the computerized signature on given hash. Mark is annexed to the information and after that both are sent to the verifier.
- Verifier sustains the computerized signature and the confirmation enter into the check calculation. The check calculation gives some an incentive as yield.
- Verifier likewise runs same hash work on got information to produce hash esteem[21,22].
- For check, this hash esteem and yield of confirmation calculation are analyzed. In view of the correlation result, verifier chooses whether the advanced mark is substantial.

Since advanced mark is made by "private" key of underwriter and nobody else can have this key; the endorser can't renounce marking the information in future.

Itthought to be seen that as opposed to marking information specifically by marking calculation, more often than not a hash of information is made. Since the hash of information is a remarkable portrayal of information, it is adequate to sign the hash set up of information. The most essential reason of utilizing hash rather than information specifically to sign is productivity of the plan. Give us a chance to accept RSA is utilized as the marking calculation. As examined out in the open key encryption section, the encryption/marking process utilizing RSA includes particular exponentiation. Marking extensive information through secluded exponentiation is computationally costly and tedious. The hash of the information is a moderately little process of the information, subsequently marking a hash is more productive than marking the whole information.

Significance of Digital Signature

Out of every single cryptographic primitive, the advanced mark utilizing open key cryptography is considered as imperative and helpful instrument to accomplish data security.

Aside from capacity to give non-disavowal of message, the advanced mark additionally gives message verification and information trustworthiness. Let us quickly perceive how this is accomplished by the computerized signature –

- Message confirmation – When the verifier approves the advanced mark utilizing open key of a sender, he is guaranteed that mark has been made just by sender who have the relating mystery private key and nobody else[23,24].
- Data Integrity – on the off chance that an aggressor has admittance to the information and changes it, the advanced mark check at collector end comes up short. The hash of changed information and the yield gave by the confirmation calculation won't coordinate. Thus, recipient can securely deny the message accepting that information honesty has been broken.
- Non-renouncement – Since it is accepted that exclusive the endorser has the information of the mark key, he can just make novel mark on a given information. Along these lines the beneficiary can display information and the advanced mark to an outsider as confirmation if any debate emerges later on. By adding open key encryption to computerized signature plot, we can make a cryptosystem that can give the four basic components of security to be specific – Privacy, Authentication, Integrity, and Non-revocation[25].

Encryption with Digital Signature

In numerous advanced correspondences, it is alluring to trade a scrambledmessages than plaintext to accomplish privacy. Out in the open key encryption conspire, an open (encryption) key of sender is accessible in open space, and consequently anybody can parody his character and send any scrambled message to the beneficiary.

This makes it basic for clients utilizing PKC for encryption to look for advanced marks alongside encoded information to be guaranteed of message verification and non-renouncement. This can filed by joining advanced marks with encryption plot. Let us quickly talk about how to accomplish this prerequisite. There are two potential outcomes, sign-then-encode and scramble then-sign.

Not withstanding, the crypto framework in view of sign-then-encode can be abused by beneficiary to parody character of sender and sent that information to outsider. Thus, this strategy is not favored. The procedure of scramble then-sign is more dependable and generally embraced. This is portrayed in the accompanying outline –

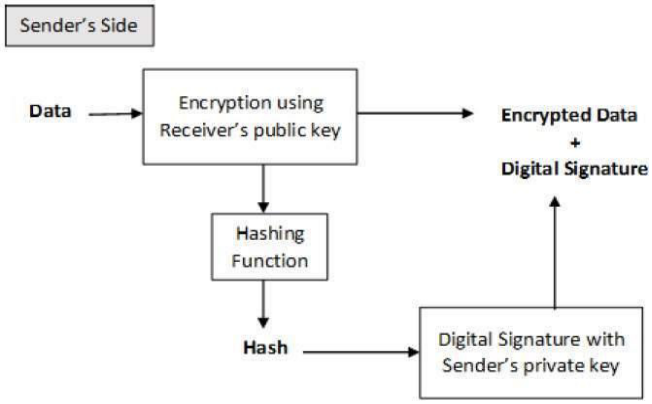

Figure 2. Structure of Digital Signature algorithm.

The collector in the wake of accepting the scrambled information and mark on it, first confirms the mark utilizing sender's open key. In the wake of guaranteeing the legitimacy of the mark, he then recovers the information through unscrambling utilizing his private key.

The RSA calculation includes four stages:

key era, key dispersion, encryption and decoding.

RSA includes an open key and a private key. The general population key can be known by everybody and is utilized for scrambling messages. The goal is that messages encoded with people in general key must be unscrambled in a sensible measure of time utilizing the private key[24,26].

RSA Implementation:

The RSA framework utilizes one route elements of a more perplexing nature. In particular, the framework utilizes measured number juggling to change a message into ambiguous cipher text. Secluded number juggling is frequently called "clock" number-crunching, in light of The RSA Algorithm was named after Ronald Rivest, Adi Shamir and Leonard Adelman, who initially distributed the calculation in April, 1977. Since that time, the calculation has been utilized in the most broadly utilized Internet electronic correspondences encryption program.

It is additionally utilized in both the Netscape Navigator and Microsoft Explorer web perusing programs in their usage of the Secure Sockets Layer (SSL), and by Master card and VISA in the Secure Electronic Transactions (SET) convention for Master card exchanges. The RSA Algorithm is just a single execution of more broad idea of open key cryptography.

Ordinary encryption strategies utilize scientific operations to change a message (spoke to as a number or a progression of numbers) into a cipher ext. Scientific operations called one way capacities are especially suited to this errand. A restricted capacity is one which is relatively simple to do in one course yet considerably harder to doefact that expansion, subtraction, and so forth, work like reading a clock.

RSA Framework:

The RSA framework utilizes increase in secluded number-crunching. The RSA framework increases one number (called the base) without anyone else's input various circumstances and the item is then isolated by a modulus. The quantity of times a base is increased independent from anyone else is known as the type and the procedure is called secluded example. 4 = (2*2*2*2) mod 12 4 = 24 mod 12 In this illustration, the number 2 is simply the base, and is increased four times, making the type the number 4 and the number 12 is the modulus.

In the RSA encryption recipe, the message M is duplicated independent from anyone else e times and the item is then separated by a modulus n, leaving the rest of a cipher text C: C = M e mod n In the unscrambling operation, an alternate type, d is utilized to change over the cyphertext once more into the plain content: M = Cd mod n The modulus n is a composite number, developed by increasing two prime numbers, p and q, together: n = p * q Also, φ(n) is known as Euler's Phi-Function and can be figured by utilizing the accompanying condition:

φ(n) = (p-1) (q-1) The encryption type e is picked with the end goal that: GCD (e, φ(n)) = 1) φ(n), an encryption type e is picked, and the unscrambling example d is figured utilizing e and φ(n). People in general encryption key is {e, n} and the private unscrambling key is {d,n}.

Encryption:

In which the message M is raised to the power e, and after that diminished modulo n, so the cipher text C can be figured as Me mod n.

Decryption:

In which the cipher text C is raised to the power d, and afterward lessened modulo, so the plaintext M is recovered utilizing the recipe, Cd mod n.

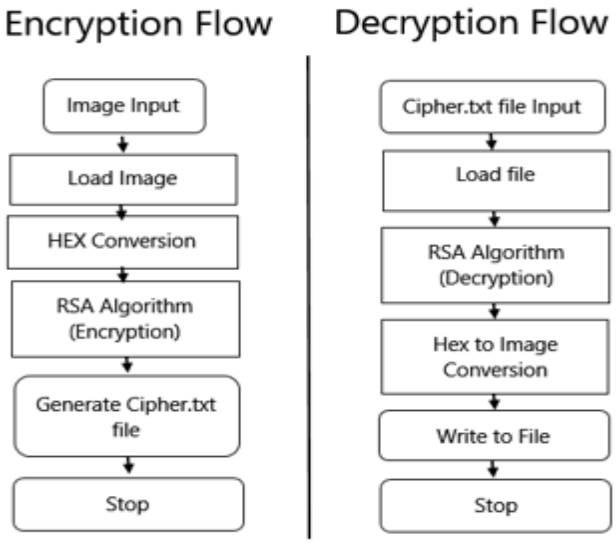

Figure 3. Flow of RSA Encryption and Decryption.

RSA Algorithm (example):

Step 1: Start

Step 2: Choose two prime numbers

p = 3 and q = 11

Step 3: Compute the value for 'n'

n = p * q = 3 * 11 = 33

Step 4: Compute the value for? (n)

? (n) = (p - 1) * (q -1) = 2 * 10 = 20

Step 5: Choose e such that 1 < e <? (n) and e and n are coprime. Let e = 7

Step 6: Compute a value for d such that (d * e) %? (n) = 1. d = 3

Public key is (e, n) => (7, 33)

Private Key is (d, n) => (3, 33)

Step 7: Stop.

Let M, is plain text (message), M= 2.

Encryption of M is: $C = M^e \% n$.

Cipher text is, $C = 2^7 \% 33$.

C = 29.

Decryption of C is: $M = C^d \% n$.

Plain text (message), $M = 29^3 \% 33$.

M= 2

Comparison table between RSA and DSA

FACTORS	**RSA(Algorithm)**	**DSA(Algorithm)**
Execution time	Slowest	Faster in signing
Key length	Based on no.of bit in N=p*q	320-bits
Block size	Variant	Variant

3. Conclusion

RSA is a solid encryption calculation that has stood an incomplete trial of time. RSA executes an open key cryptosystem that permits secure correspondences and computerized marks, and its security lays to a limited extent on the trouble of figuring vast numbers. A digital signature ensures that confidentiality, authenticity, data integrity, and undeniable of information over electronic transaction. This paper provides an comparison study of RSA algorithm and DSA algorithm in mobile cloud computing.

References

[1] W.Diffie and M. Hellman." New Directions in Cryptography". IEEE exchanges on Information Theory. IT-22(1978).472-492.

[2] R.L. Rivest, A. Shamir, and L.M. Adleman, "A technique for acquiring computerized marks and open key cryptosystems", Communications of the ACM, volume 21, pages 120-126, February1978.

[3] C. Kaufman, R. Perlman, M. Speciner, "Arrange security," Prentice Hall 1995.

[4] William Stallings, "Cryptography and Network Security Principles and Practices", fourth release, Pearson Education Inc, 2006.

[5]http://www.akadia.com/administrations/email_security.html

[6] Ronald L. Rivest, Adi Shamir, Len Adelman, "On Digital Signatures and Public Key Cryptosystems," MIT Laboratory for Computer Science Technical Memorandum 82 (April 1977).

[7] Patrick J. Flinn and James M. Jordan, Using the RSA Algorithm for Encryption and Digital Signatures: Can You Encrypt, Decrypt, Sign and Verify without Infringing the RSA Patent? Alston and Bird LLP, July 9, 1997. IJCSNS International Journal of Computer Science and Network Security, VOL.12 No.3, March 2012 82

[8] AmoghMahapatra and Rajballav Dash, "Information Encryption and Decryption by Using Hill Cipher Technique and Self Repetitive Matrix", A Thesis for the Degree of Bachelor of Technology in Electronics and Instrumentation Engineering, National Institute of Technology, Rourkela, 2007.

[9] S. Gokul, "Mixed media Magic", BPB Publications, B-14, Connaught Place, New Delhi-110001, ISBN 81-7029-9721.

[10] Dr. Ramesh Chandra Debnath and Md. Farukuzzaman Khan, "Bangla Sentence Recognition Using End-Point Detection", Rajshahi University Studies: Part B, Journal of Science, Vol 32, 2004.

[11] Udayakumar R., Kaliyamurthie K.P., Khanaa, Thooyamani K.P., Data mining a boon: Predictive system for university topper women in academia, World Applied Sciences Journal, v-29, i-14, pp-86-90, 2014.

[12] Kaliyamurthie K.P., Parameswari D., Udayakumar R., QOS aware privacy preserving location monitoring in wireless sensor network, Indian Journal of Science and Technology, v-6, i-SUPPL5, pp-4648-4652, 2013.

[13] Brintha Rajakumari S., Nalini C., An efficient cost model for data storage with horizontal layout in the cloud, Indian Journal of Science and Technology, v-7, i-, pp-45-46, 2014.

[14] Brintha Rajakumari S., Nalini C., An efficient data mining dataset preparation using aggregation in relational database, Indian Journal of Science and Technology, v-7, i-, pp-44-46, 2014.

[15] Khanna V., Mohanta K., Saravanan T., Recovery of link quality degradation in wireless mesh networks,

Indian Journal of Science and Technology, v-6, i-SUPPL.6, pp-4837-4843, 2013.

[16] Khanaa V., Thooyamani K.P., Udayakumar R., A secure and efficient authentication system for distributed wireless sensor network, World Applied Sciences Journal, v-29, i-14, pp-304-308, 2014.

[17] Udayakumar R., Khanaa V., Saravanan T., Saritha G., Retinal image analysis using curvelet transform and multistructure elements morphology by reconstruction, Middle - East Journal of Scientific Research, v-16, i-12, pp-1781-1785, 2013.

[18] Khanaa V., Mohanta K., Saravanan. T., Performance analysis of FTTH using GEPON in direct and external modulation, Indian Journal of Science and Technology, v-6, i-SUPPL.6, pp-4848-4852, 2013.

[19] Kaliyamurthie K.P., Udayakumar R., Parameswari D., Mugunthan S.N., Highly secured online voting system over network, Indian Journal of Science and Technology, v-6, i-SUPPL.6, pp-4831-4836, 2013.

[20] Thooyamani K.P., Khanaa V., Udayakumar R., Efficiently measuring denial of service attacks using appropriate metrics, Middle - East Journal of Scientific Research, v-20, i-12, pp-2464-2470, 2014.

[21] R.Kalaiprasath, R.Elankavi, Dr.R.Udayakumar, Cloud Information Accountability (Cia) Framework Ensuring Accountability Of Data In Cloud And Security In End To End Process In Cloud Terminology, International Journal Of Civil Engineering And Technology (Ijciet)
Volume 8, Issue 4, Pp. 376–385, April 2017.

[22] R.Elankavi, R.Kalaiprasath, Dr.R.Udayakumar, A fast clustering algorithm for high-dimensional data, International Journal Of Civil Engineering And Technology (Ijciet), Volume 8, Issue 5, Pp. 1220–1227, May 2017.

[23] R. Kalaiprasath, R. Elankavi and Dr. R. Udayakumar. Cloud. Security and Compliance - A Semantic Approach in End to End Security, International Journal Of Mechanical Engineering And Technology (Ijmet), Volume 8, Issue 5, pp-987-994, May 2017.

[24] Thooyamani K.P., Khanaa V., Udayakumar R., Virtual instrumentation based process of agriculture by automation, Middle - East Journal of Scientific Research, v-20, i-12, pp-2604-2612, 2014.

[25] Udayakumar R., Thooyamani K.P., Khanaa, Random projection based data perturbation using geometric transformation, World Applied Sciences Journal, v-29, i-14, pp-19-24, 2014.

[26] Udayakumar R., Thooyamani K.P., Khanaa, Deploying site-to-site VPN connectivity: MPLS Vs IPSec, World Applied Sciences Journal, v-29, i-14, pp-6-10, 2014.