IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.7, Special Issue.1, Jan 2019 E-ISSN: 2347-2693

Authentication of Study Material in E-Learning using Digital Signature Algorithms

A. Ghosh[1*], S. Karforma[2]

[1,2]Department of Computer Science, Burdwan University, Burdwan, India

[*]*Corresponding Author: ambalika_ghosh@yahoo.co.in, Tel.: +91-903390740*

Available online at: www.ijcseonline.org

Abstract—Now-a-days ICT (Information and Communication Technology) is so much improved by using various network technologies so that any type of information can be send and received very easily. This information may be belongs to banking system, government oriented system or E-learning system. Security is highly needed to protect it from any unauthorized person. For security four things are required: confidentiality, integrity, authentication and non-repudiation. When a sender wants to send an electronic document to the receiver, an attacker can get it and modify it and send the altered document to that receiver. Digital Signature is applied to avoid such situations. Properly applied Digital Signature gives confident to the receiver that the document is reliable and was sent by the original sender. Thus Digital Signature provides not only the confidentiality and integrity of the document but also provides non-repudiation so that the signature can't be denied by the signer. In this paper authors have discussed about the comparative study of different cryptographic Digital Signature algorithms such as RSA, DSA, ECDSA, GOST and ElGamal to achieve a better security for authenticity and integrity in E-Learning system during upload lecture notes between Teacher and Admin.

Keywords—ICT, Confidentiality, Integrity, Authentication, Non-repudiation, Digital Signature, RSA, DSA, ECDSA, GOST, ElGamal

I. INTRODUCTION

Now-a-days many people are using online services in different areas such as E-learning [13], E-governance, E-banking, E-commerce etc. To do so security of data and information is needed. Security is based on 4 basic components [1]:

Confidentiality- It is specifies that only the sender and the original receiver should be able to understand the content of a message. Confidentiality fails when any unauthorized person is able to access the message.

Authentication- It helps to establish the proof of identities. This process ensures that the original message is correctly identified.

Integrity- It specifies that only sender and receiver is able to change the message if they needed. An unauthorized person should not be able to modify the content of the message.

Non-repudiation- It does not allow to deny that the message is not sent by the sender. May be there is a situation when a sender sends any message but later it is refused by the sender.

The above security issues can be achieved through the implementation of various cryptographic Digital Signatures algorithms

.

The digital signature is a mathematical implementation of cryptographic technique over the digitized document to ensure its integrity and authenticity to the user. The concept of the digital signature is similar with the conventional signature which is used to verify the original document, hence the receiver can believe that the message is created by an actual sender and it is not altered or changed by an unauthorized person during the time of message passing. Thus authentication, integrity and non-repudiation of message can be achieved by the use of digital signature [5]. Many countries are already implementing different digital signature algorithms as a valid authorization technique like normal paper based signature. The digital signature algorithms, generally, has 3 sub-phases [5]-

i. Algorithm for key generation
ii. Algorithm for signature generation
iii. Algorithm for signature verification

Over the past few years many researchers have applied various techniques in the field of digital signature to achieve security- Pointchevala et al (2000) discussed some security arguments for digital signature as well as for blind signature.

Xuan et al (2009) makes the comparison of algorithms used by Digital signature in Mobile Web world. Nguyen et al (2011) describes functionality Extension of the Digital Signature Standards. Gerić et al (2012) discussed about XML digital signatures [16].

This paper helps to get an idea about the comparative study of cryptographic digital signature algorithms based on their mathematical modeling such as RSA, DSA, ECDSA, GOST and ElGamal for implementation as per their suitability during upload lecture notes in E-Learning system. Teacher upload lecture notes by signing on the document and Admin will verify the signature to assure that the note is genuine and it is uploaded by an authenticate Teacher. The remaining paper is organized as follows: in section II, authors have discussed about the different mathematical modeling of digital signature algorithms like RSA, DSA, ECDSA, GOST and ElGamal to upload lecture notes. In section III, a comparative study table is made with various parameters on the basis of the discussion in section II. Finally, in section IV, some conclusions are made to obtain suitable digital signature algorithm for uploading lecture notes.

II. MATHEMATICAL MODELLING OF DIGITAL SIGNATURE ALGORITHMS

This section describes the mathematical basis of 5 different digital signature algorithms such as RSA, DSA, ECDSA, GOST and ElGamal which are widely used now-a-days.

A. RSA

In this process modulo arithmetic is used to sign a message digitally [4]. Let Teacher (sender) sends a document to Admin (receiver). This technique considers the public key of Teacher and hash function H() is universally known. Teacher performs the following to sign a document-

Step1: Selects two prime numbers, X and Y and computes $O_{Teacher}$ = X *****Y. Then, selects $O_{Teacher}$ such that $O_{Teacher}$ has no divison (factors) in common with [(X-1) **.** (Y-1)]

Step2: Calculates the secret key $T_{Teacher}$ such that
$T_{Teacher}$ $O_{Teacher}$ = 1 mod [(X-1) **.** (Y-1)]
The public key set of Teacher contains O and $O_{Teacher}$, using which Teacher generates the signature of the document and Teacher hashes the m i.e document- [h= H(m) i.e h is the hash of the document msg]

Step3: Teacher generates the digital signature - [sign = h $T_{Teacher}$ mod $O_{Teacher}$ where sign is the signature]. Once the signature is generated, Teacher sends (m, sign) to Admin.

Step4: Admin uses the H() to obtain the h' (i.e hash'), [h' = H(m')] and Admin decrypts the signature to retrieve its hash (i.e. h), [h = sign$Q_{Teacher}$ mod $O_{Teacher}$]

Step5: Admin finally checks if : h = h'
If the match is found in the hash value retrieved and the hash value calculated, then Admin confirms the authenticity and integrity of the document along with the signature of Teacher, else it is rejected.

B. DSA

Digital Signature Algorithm [1] is quite complicated and mathematical in nature. Digital signature algorithm is generated using various domain parameters like-
A is a prime number of length I, B is a prime factor of (A-1), C= $E^{(A-1)/B}$ mod A, where E is a number less than (A-1) such that C>1,
R (private key) is a number less than B, K (public key) =C^R mod A, Message Digest algorithm is M. In our E-Learning system, Teacher (sender) wants to sign a document D and send the signed document to Admin (receiver). So it follows as:

Step1: Teacher generates a random number N, which is less than B

Step2: Teacher calculates: i) G= (C^N mod A) mod B
ii)S=(N^{-1}(M(D)+RG)) mod B, where G and S are Teacher's signature
The Teacher sends these values to Admin. Then Admin calculate the followings to verify the signature:

Step3: Q=S^{-1} mod B, T1= (M(D)*Q) mod B, T2=(GQ) mod B,
V= ((C^{T1} * K^{T2}) mod A) mod B
If V=G, then the signature is accepted else rejected.

C. ECDSA

The Elliptic Curve Digital Signature Algorithm [3, 14] is based on elliptic curve cryptography. Today this technique is highly demanding as it provides high level of security with smaller key size. To implement this, following parameters are needed-r is a prime number, c and d are integers that specify the elliptic curve equation $y^2=x^3+cx+d$, H (base point on curve)=(x_h,y_h), N is order of H such that NH=0.
Teacher generates a pair of keys using the followings-

Step1: Select a random integer e and then compute R=eH, which is a point in E_r(c,d). Here, R is Teacher's public key and e is private key.
Now Teacher is signed a document D applying the followings-

Step1: Choose a random integer l and calculate point Q=(x,y)=lH and
s=x mod N, if s=0 then goto step1

Step2: Calculate u=l^{-1} mod N and f=I(N) where I is hash function

Step3: Compute $t=l^{-1}(f+es) \bmod N$, if t=0 then goto step1
Here, s and t are signature of the document signed by Teacher.
Now Admin verify the signature using the followings-

Step1: Check s and t are integer whose range is 1 to N-1
Step2: Calculate hash value f=I(D) using proper hash function
Step3: Calculate: $W=t^{-1} \bmod N$, v1=fW and v2=sW
Step4: Calculate the point Z=(x1, y1)=v1H+v2R
Step5: If Z=0 then signature is rejected else calculate g=x1 mod N, if g=s then only Teacher's signature is accepted else not.

D. GOST

This is the Russian standard (officially called GOST R 34.10-4) [2] describing the digital signature generation and verification algorithms. It is similar to DSA and the parameters used are- A is a prime number either 509-512 bits or 1020-1024 bits, B (254-256) is a prime factor of (A-1), C is a number less than (A-1) such that $C^B \bmod A=1$, R (private key) is a number less than B and public key $K=C^R \bmod A$. This algorithm is also use a one-way hash function: M().
To sign a document D, Teacher performs the following:

Step1: Teacher generates a random number N<B , then Teacher calculates

Step2: i) $G= (C^N \bmod A) \bmod B$, ii) $S= (RG+N(M(D))) \bmod B$
If M(D) mod B=0, then it equals to 1 and If G=0 then select another N to start again. The two number signatures are generated: G mod 2^{256} and S mod 2^{256} that are send to Admin.

Step3: Admin verifies the signature by calculating- $Q=M(D)^{B-2} \bmod B$, T1=(SQ) mod B, T2=((B-G) *Q) mod B, $V=((C^{T1} * K^{T2}) \bmod A) \bmod B$
If V=G then the signature is accepted, otherwise not verified.
The main difference with DSA is that, in DSA S= $S=(N^{-1}(M(D)+RG)) \bmod B$ that specify a different verification calculation. Here B is 256 bits while others satisfied with 160 bits.

E. ELGAMAL

ElGamal digital signature [1, 15] is the asymmetric approach of authentication mechanism based on discrete logarithm problem in a finite field [4]. To perform digital signature, some parameters are used- A is a prime number, C and R are another random numbers, both are less than A, other than A and C, public key $K=C^R \bmod A$ where R is the private key [1].

Now Teacher wants to send a signed document D to Admin. Teacher perform the followings to generate signature [2]-

Step1: Teacher generates a random number N that is relatively prime to A-1.

Step2: Teacher now calculates: i) $G=C^N \bmod A$,
ii) S such that D=(RG+NS) mod (A-1)
Values G and S are the sender's signature and N must kept secret. Now the signature is verified by Admin if the following holds-

Step3: $K^G G^S \bmod A=C^D \bmod A$, if the match is found, Admin then confirms the authenticity and integrity of the Teacher's document.
Each ElGamal signature needs a randomly chosen value of N.

III.TABLE OF COMPARATIVE STUDY

The authors are able to make comparative study [6, 7, 8, 9, 10, 11, 12, 17, 18, 19, 20, 21] of the above mentioned digital signature algorithms with the help of various aspects as shown in given Table1.

Parameters	RSA	DSA	ECDSA	GOST	ElGamal
Published Year	1977	1991	1992	1994	1985
Designer	R. Rivest, A. Shamir, L. Adleman	NIST(National Institute of Standards and Technology)	Scott Vanstone	Russian Federation	Taher ElGamal
Type	Asymmetric	Asymmetric	Asymmetric	Symmetric	Asymmetric
Key Size	1024 to 4096 bit	192 bit	160 bit	256 bit	>1024 bit
Block Size	Depend on key size	256 bit	320 bit	64 bit	Depend on key size
Based On	IFP(Integer Factorization Problem)	DLP(Discrete Logarithm Problem)	ECDLP(Elliptic Curve Discrete Logarithm Problem)	Operations with an elliptic curve points group, defined over a prime finite field	DLP(Discrete Logarithm Problem)
Application Area	i. PC, Laptop, Super computer ii. Widely used in industry	i. Protecting data transfer using SSL/TLS ii. Protecting mail using S/MIME or PGP	i. Any light weight device ii. Mobile framework iii. Sensors iv. Wireless system	i. Data transmission via insecure public telecommunication channel ii. Use for public service in Russian Federation	i. Latest version of PGP ii. GNU Privacy Guard software
Speed	Slow	Fast	Faster than RSA, DSA	Slower than DSA	Very Fast
Security	Secure	Secure	Highly Secure	Not secure in theoretical sense	Secure
Advantages	i. Easy to understand	i. Efficient for	i. Key size is shorter	i. Recommended for creation,	i. Shorter key size is

	and implement ii. Encryption and verification is fast iii. Widely used in industry	decryption and key generation ii. Essential for secure transaction over open network iii. Less storage space is required	ii. Requires less storage space iii. Provides faster computation iv. Provides greater security	operation and modernization of data processing system ii. Suitable to extended signature concept i.e. for multi signature or blind signature	required ii. Efficient for decryption process iii. Offers high strength level
Disadvantages	i. Requires large key size ii. Key generation ,decryption and signing is slow	i. Encryption and verification is slow ii. Complicated than RSA	i. Little bit slower for encryption and signature verification ii. Little complicated to understand	i. 1.6 times slower than DSA	i. Computation process requires longer time ii. Not so popular as it is new in market
Attacks	Timing Attack	Correlation Power Analysis Attack	Fault Attack	Differential Attack	Forged Signature Attack

IV. CONCLISIONS

This paper presents study of mathematical modeling of 5 important digital signature algorithms at a glance, so that user is able to understand appropriate algorithm is suitable to implement during upload lecture notes to ensure authenticity and integrity. All algorithms have their own benefits and limitations. DSA is secure but not efficient for signature verification. GOST can be implemented but it is slower than DSA. On the other hand, RSA is secure but it requires larger key size which increases complexity that is the reason to use ElGamal cryptosystem. Again it requires longer computation time. Now it is replaced by Elliptic curve [6]. ECDSA provides high level of security with smaller key size. As it is new in market, the application of elliptic curve versions become very popular among the researchers [4]. They will make primary choice of applying elliptic curve on different standard digital signature algorithms like ECRSA, ECDSA, EC-ElGamal etc. in near future to achieve high security.

REFERENCES

[1] A.Kahate, "*Cryptography and Network Security*", McGraw-Hill Publisher, India, pp.7-9,197-199, 2010.

[2] B. Schneier, "*Applied Cryptography*", Wiley Publisher, India, pp. 476-478,495-496, 2007.

[3] W. Stallings, "*Cryptography and Network Security Principles and Practices*", Pearson Publisher, India, pp.398-400, 2012.

[4] A. Roy, S. Karforma, "*A Survey on digital signatures and its applications*", Journal of Computer and Information Technology Vol. 03 , No. 1 & 2, Pp- 45-69, August 2012.

[5] A. Ghosh, S. Karforma," *Object Oriented Modeling of DSA for Authentication of Student in E-Learning*", International Journal of Science and Research, Vol. 03, No. 07, pp. 2293-2297, July 2014.

[6] M. Kaur, N.Kaur, B. Singh, "*Comparative Study of Different Cryptographic Algorithms*", International Journal of Advanced Research in Computer Science, Vol. 8, No. 4, pp. 352-354, May 2017.

[7] C. Endrodi, "*Efficiency Analysis and Comparison of Public Key Algorithms*", Presented in Conference of PhD Students in Computer Science, July 2002.

[8] A. Sarkar, "*An Overview of Cryptographic Algorithms and Security Challenges in Big Data*", ACCENTS Transaction on Information Security, Vol. 1, pp. 7-14, 2016.

[9] R. Haddaji, R. Ouni, S. Bouaziz, A. Mtibba, "*Comparison Digital Signature Algorithm and Authentication Schemes for H.264 Compressed Video*", International Journal of Advanced Computer Science and Applications, Vol.7, No. 9, pp.357-363, 2016.

[10] A. Khalique, K. Singh, S. Sood, "*Implementation of Elliptic Curve Digital Signature Algorithm*", International Journal of Computer Applications, Vol. 2, No. 2, pp. 21-27, May 2010.

[11] A. I. Ali, "*Comparison and Evaluation of Digital Signature Schemes Employed in NDN Network*", International Journal of Embedded Systems and Applications, Vol. 5, No. 2, pp. 15-29, June 2015.

[12] M. Michels, D. Naccache, H. Petersen, "*GOST 34.10- A Brief Overview of Russia's DSA*", Published in Computers and Security, Vol. 15, No. 8, pp. 725-732, 1996.

[13] E. R. Weippl, "*Security in E-Learning*", Springer Publisher, India, 2005

[14] D. Johnson, A. Menezes, S. Vanstone, "*The Elliptic Curve Digital Signature Algorithm (ECDSA)*", International Journal of Information Security, Vol. 1, No. 1, pp. 36-63, 2001.

[15] S. Karforma, S. Banerjee , "*Object Oriented modeling of ElGamal Digital Signature for authentication of study material in E-learning system*", IJARSE, Vol..4, No.2, pp. 455-460 February 2015.

[16] S. Singh, Md. S. Iqbal, A. jaiswal, "*Survey on Techniques developed using Digital Signature: Public Key Cryptography*", International Journal of Computer Applications, Vol. 117, No. 16 pp. 1-4, May 2015.

[17] A. H. Lone, M. Uddin, "*Common Attacks on RSA and its Variants with Possible Countermeasures*", International Journal of Emerging Research in Management & Technology, Vol. 5, No. 5, pp. 65-70, May 2016.

[18] M. Repka, M. Varchola, M. Drutarovsky, " *Improving CPA Attack Against DSA and ECDSA*", Journal of Electrical Engineering, Vol. 06, No. 03, pp. 159-163, 2015.

[19] J. Schmidt, M. Medwed, "*A Fault Attack on ECDSA*", In the Proceedings of the 2009 workshop on Fault Diagnosis and Tolerance in Cryptography, Lausanne, Switzerland, pp. 93-99,2009.

[20] N. Courtois, M. Misztal, "*1st Differential Attack on Full 32-Round GOST*", International Conference on Information and Communications Security, Beijing, China, pp. 216-227, 2011.

[21] X. Li, X. Shen, H. Chen, "*ElGamal Digital Signature Algorithm of Adding a Random Number* ", Journal of Networks, Vol. 06, No. 05, pp. 774-782, May 2011.

Authors Profile

Prof. Sunil Karforma- has completed B.E. (Computer Science and Engineering) and M.E. (Computer Science and Engineering) from Jadavpur University. He has completed Ph.D. in the field of Cryptography.

He is presently holding the post of Professor as well as Head of the Department in the Department of Computer Science, The University of Burdwan. Network Security and E-commerce is his field of interest in research area. He has published research papers in reputed National and International journals and proceedings.

Ms. Ambalika Ghosh- has completed BCA (H) and MCA from Burdwan University and WBUT respectively. Presently she is enhancing her knowledge sphere as Research Scholar in The Department of Computer Science under The University of Burdwan, Burdwan and has published few research papers in standard national and international proceedings and journals. She is presently holding the post of Assistant Professor in Swami Vivekananda Institute of Modern Science, Kolkata. Before joining SVIMS, she worked in BIMS as Lecturer and Keane India Ltd. as Software Engineer. The area of her research interest is in Network Security, Cryptography and E-learning.

