A STUDY AND ANALYSIS OF AUTHENTICATION AND DIGITAL SIGNATURE USING PUBLIC KEY, PRIVATE KEY PAIR

Upendra,Manu Vardhan,Pinkesh Narad
Assistant Professor
Department of CSE
National Institute of Technology, Raipur,India

Abstract: *Cryptography* is plays an important role to protect data and information in world wide web. In this paper we present a detailed study of open message format and secure message format with their strengths and weaknesses over each other based on their security service goal. we also focus on asymmetric cryptography to perform encryption and decryption operations using public key, private key pair in order to archive most important security services to the sender like authentication,confidentiality,digital signature and non-repudiation.We have also provided a fair comparison between most common asymmetric key cryptography algorithms: RSA and Diffie-hellman algorithm.

IndexTerms – Cryptography, Asymmetric key algorithm, Digital Signature, Authentication, RSA,Diffie Hellman Algorithm

I. INTRODUCTION

Cryptography is playing very important role to protect information transmitted over a wireless or wire communication channel [1].there are two methods. One is symmetric and other one is asymmetric key cryptography.

Symmetric key Cryptography deal with same key, if client have plain text then we have something called as encryption algorithm, and to this encryption algorithm ,we generally provide something called as key ,now this encryption algorithm is going to convert plain text into cipher text, and now this cipher text, we will be sent on the wire, to the other side, now the other side is going to take this cipher text and this cipher text will be given to something called as decryption algorithm and to decrypt it again the same key, which ever sender used the same key will be use that is called as symmetric means same thing and shared key

1.1 Authentication using public key private key:

How to use public key, private key for Authentication and Digital Signature. Say Authentication means for example here two person Ana and Brat. Here suppose you are Ana and it is Brat.you have send an email to your bank, bank saying that, you want to transfer some amount to your friend's account, according to your order,They have transferred the money to your friends account, later you can go to the bank and you can say that I have never send to an email ,someone else have send that email. Then how can be bank prove that, it is you, who has send the email. earlier when, you are doing transfer using the cheque used to have the signature, So maybe you have some signature on the cheque and from this signature, it will be authenticated that is you are the person who has given the orders but now, when you are sending the orders through the email. No way you can do the authentication, So for that reason, we needs something called as digital signature.

So digital signature is signature using some other means, so that it can be applied for this ecommerce. How to use the public key, private key encryption in order to get digital signature? Now see this whenever Ana is going to send a message, the other party should be very sure that it is Ana who has send the message and not anyone else, so whenever Ana is going to send the plain text. Ana is going to encrypted and for this encryption, we have three choices, what are all possibilities that Ana has? so one choice is, it can use its public key, other choice is, it can use its private key and other is, it can use the other party's public key, if it uses its public key then we can never be sure that the message is originating from itself Ana because everyone has public key of Ana. So anyone can send it using public key of Ana, May be, and more ever this same thing apply to this also. Everyone has public key, so if we have to be sure that the message is originating from Ana,It has to be encrypted with something which only Ana has. Now what is Ana has? The private key of Ana. So if Ana is going to encrypted using its private key(Pr_A),Then the receiving party will be very sure that, the message is originating from Ana itself, because only Ana has its own private key,

Now, we are going to get this cipher text and this cipher text is going to be send the other side and this cipher text is going to be decrypted and future decryption what key should be used? It is encrypted using private key(Pr_A) of Ana and whenever we use the private key of Ana to encrypted the only way to decrypted using the public key(Pu_A) of Ana. Brat have the public key(Pu_A) of Ana to get the plain text then we can be very sure that, it is encrypted using private key(Pr_A) of Ana, otherwise this could not have been possible and so who has a private key(Pr_A) of Ana, only Ana, therefore we can sure that the message is coming from Ana,so using this method authentication can be verified which means sender side indent can be verified, so what they will do, in order to save digital signature they will take this plain text and they save the copy of both of them, if you ever complaint them that you are not that who has send, then they show that, see this is cipher text we got and from this got plain text in order to converted we have used your public key, therefore your private key must have been used, so your private key is supposed to be sucured.only you know it. therefor it has come from you, there is no way it must have been sent from anyone else, got it, using this method, this cipher text is called as Digital signature.so if you save a copy of cipher text called as digital signature the entire procedure used for authentication, you can save the digital signature and now using this method we are able to provide only authentication. Not the security, this sense since you are sending the message encrypted using private key(Pr_A) of Ana, anyone on the way can even get the message and converted it into the plain text using public key(Pu_A) of Ana because public key of Ana is well known to every one.therefore this method is used only to provide the authentication and not for security.so anyone can open the message, see it but anyone the entire method is authentication, not about security.

Second option private key of Ana (Pr_A).if Ana uses its private key(Pr_A),what happens anyone who has public key(Pu_A) of Ana can open it and who has it? Everyone, therefore no need to encryption at all, if you are just going to encrypted a message using private key of Ana.

Any one sending it without any encryption, therefore it is better that you, send it using public key of Brat, if you are sending then who can open it, whoever has private key of Brat, only Brat. If I use public key of Brat to encrypt the message, then who can open it, only the person has private key of Brat and who has a private key of Brat, Brat itself, therefore if i use public key(Pu_B) of Brat, only Brat can decrypt it, so I am going to use public key Brat for encryption, so that only Brat can open it.Now I get the cipher text

1.2 Encryption using public key private key:

There are two parties one is Ana, other is Brat. If Ana wants to send information to Brat securely, before doing this both Ana & Brat are supposed to generate a pair of keys known as public key and private key, So Ana is going to generate a pair of known as private key of Ana and public key of Ana, Brat is going to generate one pair of key known as private key of Brat & public key of Brat. Now this two keys in such a way that once we encrypt anything using public key of Ana Then we can decrypted only using private key of Ana, if encrypt anything using private key of Ana, we can decrypt using only public key of Ana, and same thing is true with this. If encrypt anything using public key of Brat then only decrypt using private key of Brat, if we encrypt anything using private key of Brat, Then decrypt using only public key of Brat. Public key of Ana & public key of Brat are kept known globally which means everyone should, what public key of Ana & Brat. Before start the communication both Ana & Brat supposed to generate pair of keys. This pair of keys should be such in way that, if encryption is done with one of them, Then decryption should be done with other one. We can call one of them as private key, other one as public key. The reason behind it is public key is going to be known globally and private key will be known only that party. Private Key of Ana will be known only to Ana and no one else will be known it, and more ever given this public key, no one able to find out what is private key. So that is known private key, private means no one known about it, Public key means every one known about it. so public key of Ana, everyone known about it, private key of Brat, only Brat known about it, no one else about known it.

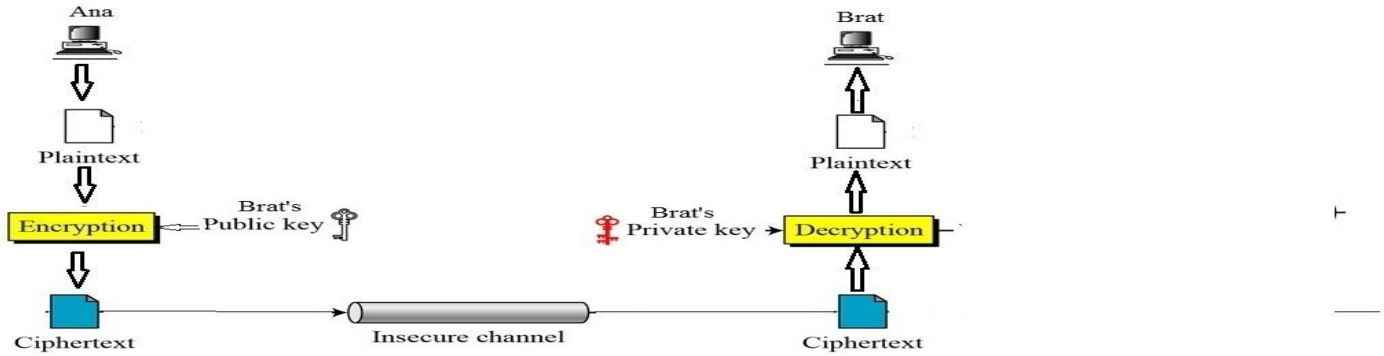

Figure 1: Encryption using public key private key

II. RELATED WORK

We have two types of cryptography one is called symmetric key cryptography or shared key or "secret key", use the *exact* same key for both encryption and decryption [17][19] other is called asymmetric key cryptography or public key private key cryptography.

Asymmetric key encryption algorithms also known as "public key" cryptography is a form of modern cryptographic in which encryption process and decryption process depend on complex algebraic, algorithmic, numerical theory performed using two different keys, one key is private key and the other is referred to as public key. Some famous and well known asymmetric key encryption algorithms like PGP, with versions using RSA [16][17] and Diffie-Hellman [18], Secure Shell (SSH) provides strong encryption and integrity protection [6],Elliptic Curve Cryptosystem(ECC),Digital Signature Algoritm(DSA)[21], Merkle-Hellman Knapsack, ElGamal. Asymmetric key cryptography uses twopair of keys one is public which means everyone known and private key generated by asymmetric algorithm for protecting encryption keys and key distribution, and a secret key is generated by a symmetric algorithm and used for bulk encryption[22]. Emmanuel Bresson et al. [2] has investigated the Group Diffie-Hellman protocols for authenticated key exchange.

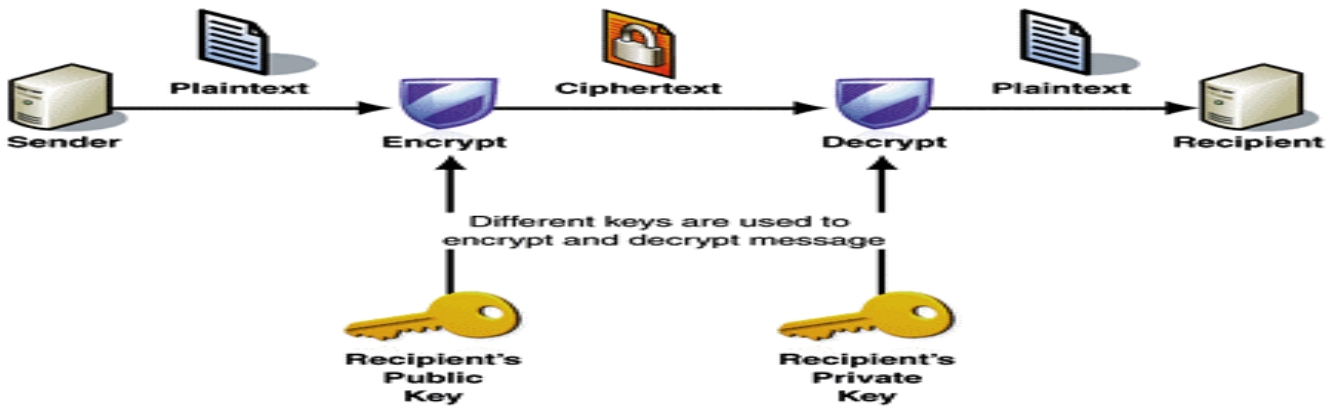

Figure 2: Asymmetric Key Cryptography

Encryption and authentication using public key private key:
Ana is going to have plain text, now plain text will be taken by Ana and it will be encrypted and for this encryption, what should be key? So Ana wants to do both the thing, Ana wants to provide security that encryption part and other is digital signature, for that encryption part if only Brat has to be open it. Ana uses public key of Brat (Pu_B) so that Brat can open it then Ana will get cipher text, call this CT-1 and this CT-1 will again be encrypted for this encryption, now Ana wants to send digital signature or Ana wants to purposes authentication for that reason. Ana is going to again encrypted using its private key(Pr_A).Now Ana is going to both the key one after the another, Now Ana is going to get cipher text-2,call this CT-2,Now this CT-2 ,will be transferred on the way, even if this has been seen by anyone, not will be open it.This will be decrypted first, so here, There is CT-2,Now CT-2 will be decrypted, Now for this decryption, what should be the key? on the other side, the last key is used this private key of Ana(Pr_A).Therefore Brat is going to public key of Ana as first key for decryption, whatever is used to last ,So we used first. Brat is going to get cipher text(CT-1) and again this cipher text(CT-1) has to be decrypted and for this decryption, What should be used, Brat has use its public key(Pu_B) and other side, Therefore Brat used its private key(Pr_B).private key(Pr_B) of Brat, Brat has it, and public key(Pu_A) of Ana, Brat has it. Finally going to get plain text ,and this is going to give Brat, So how is security is implemented, security is implemented because, only Brat can open it, How is the Digital Signature known implemented, So What will be Digital signature.in this case, in order to save digital signature they have to take the plain text and digital signature is going to be CT-2,now this CT-2 has been decrypted only using your public key, therefore CT-2 has been encrypted using your public key. Both for encryption as well as authentication, here Ana is using public key of Brat first and then public key of Ana. It need not be same that

III. COMPARISON

Following table presents comparison of RSA and Diffie-Hellman algorithm on the basis of standard parameter:

TABLE I. COMPARISON TABLE FOR DIFFERENT SYMMETRIC KEY ALGORITHMS

Algorithm	Created by	Block Size(bits) or Plain/Cipher Text Length	Key Size or Length (bits)	Number of Rounds	CIPHER TYPE	Structure	Possible Attacks	Strength	Weakness
RSA	Rivest, Adi Shamir and Leonard adleman In 1977	Depends on key size	>1024 bits	1 round for each message	Block cipher	Common network	Timing attack	public key, Secures digital signatures	slower
DIFFIE-HELLMAN	whitfield diffie and martin hellman1976	64bits	uses key exchange manage ment	14	symmetric key cipher	Common network	Eaves dropping	hard to solve discrete algorithm,doe s not transmit shared key through the channel	No authenticati on

IV. Conclusions

This paper provides performance analysis of different Asymmetric encryption algorithms. The Algorithms have been presented and comparison shows that some parameters like algorithm key size, block size, cipher type, number of rounds, possible attacks are playing an important role to achieve the goal of security services provided by Asymmetric Cryptography. We conclude that RSA performs better encryption in comparison to Diffie-Hellman algorithm.

REFERENCES

[1] Sumedha Kaushik &Ankur Singhal "Network Security Using Cryptographic Techniques," International Journal of Advanced Research and Computer Science and Software Engineering, Volume 2, Issue 12, December 2012.18
[2] Dr. Prerna Mahajan &Abhishek Sachdeva "A Study of Encryption Algorithms AES, DES and RSA for Security," Global Journal of Computer Science and Technology Network, Web & Security, Volume 13 Issue 15 Version 1.0 Year 2013
[3] Dr. Prerna Mahajan & AbhishekSachdeva "A Study of Encryption Algorithms AES, DES and RSA for Security," Global Journal of Computer Science and Technology Network, Web & Security, Volume 13 Issue 15 Version 1.0 Year 2013
[4] O.P Verma, RituAgarwal, DhirajDafouti and ShobhaTyagi, "Peformance Analysis Of Data Encryption Algorithms",IEEE Delhi Technological University, India,2011.
[5] Data Encryption Standard, Federal Information Processing Standard (FIPS) Publication 46, National Bureau of Standards, U.S. Department of Commerce, Washington, DC ,January 1977.
[6] Text Book: Cryptography and network security, Principles and practices by William Stalling, Retrieved on 8 December 2006
[7] Federal Register: September 12, 1997 ,Volume 62, Number 177.
[8] Federal Register: September 14, 1998 ,Volume 63, Number 177.
[9] X. Lai and J. Massey "A proposal for a new block encryption standard", In Proceedings of the EUROCRYPT 90 Conference, pp. 3 89-404, 1990.
[10] Wheeler, D.J., & Needham, R.J. (1994), "TEA, a tiny encryption algorithm" In Fast Software Encryption – Proceedings of The 2nd International Workshop,1008
[11] Schneier et al., Twofish: A 128 bit Block Cipher, AES algorithm submission, June 15, 1998
[12] AES home page may be found via http://www.nist.gov/ CryptoToolkit.

[13] J. Daemen and V. Rijmen, AES Proposal: Rijndael, AES algorithm submission, September 3, 1999,
[14] James Nechvatal, Elaine Barker, Lawrence Bassham, William Burr, Morris Dworkin, James Foti, and Edward Roback, Report on the Development of the Advanced Encryption Standard (AES), Volume 106 Number 3 May– June 2001
[15] Federal Register: January 2, 1997 ,Volume 62, Number 93
[16] Rivest, R.L., Shamir, A., Adleman, L. "A Method for Obtaining Digtal Signatures and Public Key Cryptosystems," Communications of the ACM, 21, No. 2, 120-126 (1978).
[17] RohitMinni, KaushalSultania, Saurabh Mishra, and Prof Durai Raj Vincent, "An Algorithm to Enhance Security in RSA", *4th ICCCNT 2013*, pp. 1-4, IEEE
[18] Diffie, W. and Hellman,M.E., "New Directions in Cryptography", IEEE Transactions on Information Theory, IT-22, No. 6, 644-654 (1976).
[19] Bruce Schneier, "The Blowfish encryption algorithm9", Dr. Dobb's Journal of Software Tools, 19(4), p. 38, 40, 98, 99, April 1994.
[20] Heys, H.M.; Tavares, E. "On the Security of the CAST Encryption Algorithm", Electrical & Computer Engg.
[21] Rivest, R.L., Shamir, A., Adleman, L. "A Method for Obtaining Digtal Signatures and Public Key Cryptosystems," Communications of the ACM, 21, No. 2, 120-126 (1978).
[22] www.webopedia.com/TERM/S/symmetric_key_cryptography.html
[23] Schneier et al., Twofish: A 128 bit Block Cipher, AES al-gorithm submission, June 15, 1998.
[24] Emmanuel Bresson, Olivier Chevassut, David Pointcheva, Jean- Jacques Quisquater, "Authenticated Group Diffie-Hellman Key Exchange", Computer and Communicatio n Security- proc of ACM CSS'01, Philadelphia, Pennsylvania, USA, Pages 255-264, ACM Press, November 5-8, 2001.