International Journal of Current Advanced Research
ISSN: O: 2319-6475, ISSN: P: 2319-6505, Impact Factor: SJIF: 5.995
Available Online at www.journalijcar.org
Volume 6; Issue 8; August 2017; Page No. 5359-5362
DOI: http://dx.doi.org/10.24327/ijcar.2017.5362.0706

Research Article

KEY AGREEMENT PROTOCOLS & DIGITAL SIGNATURE ALGORITHM

Shafiqul Abidin*

Department of Information Technology, HMR Institute of Technology and Management,
GGSIP University, Delhi, India

ARTICLE INFO

Article History:

Received 10th May, 2017
Received in revised form 5th
June, 2017 Accepted 16th July, 2017
Published online 28th August, 2017

Key words:

Key agreement; digital signature standard; Diffie-Hellman protocol; public-key cryptography; random numbe; Diffie Hellman exchange algorithm.

ABSTRACT

Diffie-Hellman have contributes lot in encryption. The most commonly used algorithm of Diffie Hellman is – Key Exchange Algorithm. This algorithm is used to exchange keys through a network. But Diffie Hellman key exchange algorithm has flaws and shortcomings. I have made an effort to propose a new key agreement protocol that combined the features of key confirmation and Diffie Hellman. Whitfield Diffie and Martin Hellman proposed first public key algorithm. This is called Diffie - Hellman algorithm and provided communication between two public channels. This is useful even without knowing each other. This algorithm provides a platform for communication over insecure channels. This is supposed to be the first public-key protocol. After implementing the said protocol it was incorporated with digital signature algorithm. In this research article effort is being made to present the verification of digital signature standard with respect to Diffie-Hellman. This algorithm is being implemented by selecting two integers in random fashion. This article will show that by using this protocol that the utmost secrecy can be maintained. Further freshness of key remain intact even after continuous selecting random numbers. A new protocol on the basis of key confirmation and Diffie-Hellman is also being proposed. This protocol is equally useful on the elliptic curve cryptography in asymmetric encryption.

INTRODUCTION

Earlier a scheme was introduced by Arazi for the integration of Diffie-Hellman key exchange protocol with digital signature [1]. Thereafter a scientist named Harn *et.al.* have added a milestone improvement in the algorithm. Now this algorithm is capable of preventing known and unknown attacks - key attack, key relay attack etc [2]. Phan presented his paper with addition of two important attributes that is forward secrecy and freshness of keys [3]. To make a communication between two channels, the session keys are mandatory. These session keys are generated by the key agreement protocol. The first key agreement protocol was introduced by Diffie-Hellman and the protocol was solely based on asymmetric encryption or public key cryptography [4]. Diifie-Hellman introduced two versions of protocol. In their first version all the entities in the communication network exchange the static public keys. The shortcoming of first version was that the same session keys were generated for each run of protocol. In other version they exchange the ephemeral public keys which is vulnerable to the man-in-middle attack. To overcome these a protocol based on authenticated key agreement is introduced. Which combines freshness of keys and randomly selected number has been introduced in this paper. This protocol is being verified with the digital signature standard [6].

Related Work

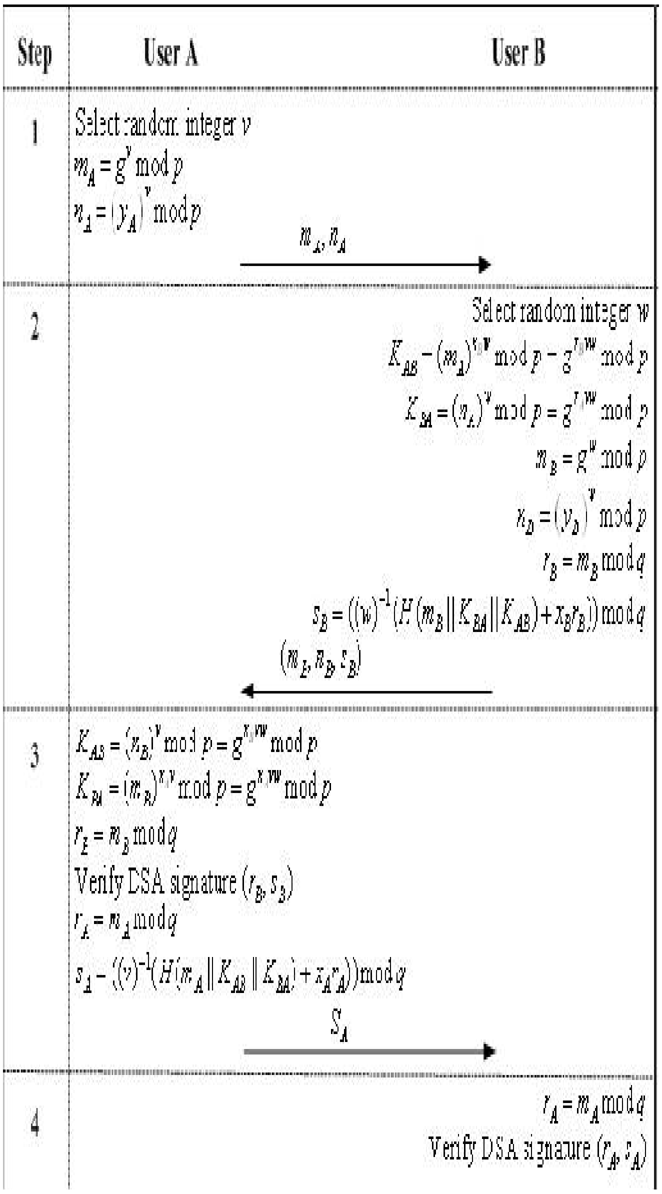
For this protocol we need to know that two publicly known numbers i.e. p and g which will be the primitive root of p. Suppose there are two users A and B which want to exchange a key and unknown to each other. First time user A select a random Integer X_A <p and compute $Y_A = g^{XA} \bmod p$. Similarly, user B selects a random number X_B <p and computes $Y_B = g^{XB} \bmod p$. Each side keeps the value of X privately and make the Y value available publicly to the other side so this is called public key for both of users A and B and the process is known as the public key generation for A and B [7]. Now user A computes the key as $K= (Y_B)^{XA} \bmod p$ and user B computes the key $K= (Y_A)^{XB} \bmod p$. These two values should produce similar result.

$$K = (Y_B)\ X_A \bmod p$$
$$= (g\,^{X}_{B} \bmod p)\,^{X}_{A} \bmod p$$
$$= (g\,^{X}_{B})\,^{X}_{A} \bmod p \quad \text{By the rule of modular arithmetic.}$$
$$= g^{X} B^{X}_{A} \bmod p$$
$$= (g\,^{X}_{A})\,^{X}_{B} \bmod p$$
$$= (g\,^{X}_{A} \bmod p)\,^{X}_{B} \bmod p$$
$$= (Y_A)\,^{X}_{B} \bmod p$$

Corresponding author:* **Shafiqul Abidin
Department of Information Technology, HMR Institute of Technology and Management, GGSIP University, Delhi, India

The result shows that the two sides can change the secret value and both values are identical with each other.

Phan [8] integrated these computation used in Diffie-Hellman key exchange protocol in to Digital Signature algorithm as follows.



Step	User A	User B
1	Select random integer v $m_A = g^v \bmod p$ $n_A = (y_A)^v \bmod p$ $\xrightarrow{m_A, n_A}$	
2		Select random integer w $K_{AB} - (m_A)^{x_B w} \bmod p - g^{x_B vw} \bmod p$ $K_{BA} = (n_A)^w \bmod p = g^{x_A vw} \bmod p$ $m_B = g^w \bmod p$ $n_B = (y_B)^w \bmod p$ $r_B = m_B \bmod q$ $s_B = ((w)^{-1}(H(m_B \| K_{BA} \| K_{AB}) + x_B r_B)) \bmod q$ $\xleftarrow{(m_B, n_B, s_B)}$
3	$K_{AB} = (n_B)^v \bmod p = g^{x_B vw} \bmod p$ $K_{BA} = (m_B)^{x_A v} \bmod p = g^{x_A vw} \bmod p$ $r_B = m_B \bmod q$ Verify DSA signature (r_B, s_B) $r_A = m_A \bmod q$ $s_A - ((v)^{-1}(H(m_A \| K_{AB} \| K_{BA}) + x_A r_A)) \bmod q$ $\xrightarrow{S_A}$	
4		$r_A = m_A \bmod q$ Verify DSA signature (r_A, s_A)

Proposed Work

The proposed system works as follows there are the following notations which we have used in the protocol.

A,B	Entities
ID_A, ID_B	Identity parameter of A,B
G	Generator Point
$E_k(x)$	Encryption of x using the key k
$D_k(x)$	Decryption of x using the key k
KR_A	Static private key of A
KU_A	Static public key of A which is elliptic curve point i.e. KRA.G
r_A	A's ephemeral key (Random no.)
K	Session key between entities
A→B: M	Sending of message M From A to B
Sgn_A	Signature using private key of A
SK	Session key between A and B

For B we have similarly KR_B, KU_B, and r_B

The proposed protocol works on the domain parameter of elliptic curve that are common to both entities and cover an elliptic curve E defined over a field Fq which is generating a point G of elliptic curve cryptography so that G belongs to E (Fq), n is order of G in E (Fq), and h is cofactor of n [9].

The above integration done by the Phan was for authenticated key distribution. We only review and analyze the work done by Phan and tried to prove the correctness of digital signature standard algorithm with the integration of Diffie-Hellman key exchange protocol. In the DSS approach of digital signature we have the integration with Diffie-Hellman a protocol as follows.

The hash code is provided as input to a signature function along with a random number (can be selected as randomly as we did in Diffie-Hellman algorithm) K is generated for signature. This signature function also depends upon the sender A's privately selected key X_A and globally selected integer g [10].

If the result of digital signature consists of two component s and r then the output of the verification function is a value that will be equal to the value considered in sighing function 'r' if signature is valid [11].

Suppose there are three parameters (public key elements) p, q, g.
Where
p is a prime number selected with a length bit 512 & 1024 bit. i.e.

$512 \leq L \leq 1024$ & L is multiply of 64
q divides (p-1) & bit length 160 bits (160 prime number)
g is the h (p-1) / q mod p where h is any integer.

Now user select a private random integer number as in Diffie-Hellman protocol X_A <p by this we can generate the user's public key Y_A = g X_A mod p. [12] In the DSS approach user can select a per-message secret number k which is randomly selected by any algorithm of random number generation also known as the nonce but it should be 0 < k <q.

Signing function:

$$r = (g\ k \bmod p.) \bmod q$$
$$s = [K\text{-}1\ H(M) + X_A r] \bmod q$$

Signature will be (r, s)

Verifying function:

$$w = (s')^{-1} \bmod q$$
$$v_1 = [H(M')\ w] \bmod q$$
$$v_2 = (r')\ w \bmod q$$
$$r' = [(g^{v1}\ Y_A{}^{v2}) \bmod p] \bmod q$$

Where M = Message to be signed
H (M) = Hash of using SHA-1
M' r's' = Received version of M, r, s.

For the establishment of any session the entities need a session key and for sharing of a session key they should know the public key of each other this process can be done by the certificate authority[13] which provides CAA i.e. A's certificate congaing the public key and the signature of A. the proposed protocol will work as follows.

The communicating entities will take the public keys of each other with the help of certificate authority. Now A will have KU_B and B will have $KU_{A[14]}$.

The session key K will be generated by using the KRA and KU_B as K = KR_A.KU_B = KR_A.KR_B.G

In the next step a select a random number rA as its ephemeral key and computes a point on elliptic curve MA = rA KU_B. After encryption of signed message with K the result is like.

A→B: $ID_B, E_K(M_A, Sgn_A\ (ID_B, KU_A, KU_B))$

With the same process like A,B will also find the value of K, and decrypts the message received from A, recovers MA and verify the signature sent by A.B will select again a random number rB as its ephemeral key and calculate the session key SK = h(rB KU_A + MA). If SK = 0 then B can terminate the protocol. Otherwise B will send a message to A as A did in previous step.i.e.

B→A: $E_K\,(M_B)$, $E_{SK}\,(Sgn_B\ (ID_A,\ M_A,\ M_B))$

After receiving the message from B, A decrypts with K to recover MB. The session key will be computed again with the help of KU_B and MB if SK = 0 then A will terminate the protocol otherwise a message will be sent to B [15].

A→B: $E_{SK}\,(Sgn_A\ (ID_A,\ M_A,\ M_B))$

In the last step B will decrypt the received message using SK and verify the signature created by A. if the signature verified then B will store the session key SK. The multiplication by h in SK will ensure that the session key SK is a point in the subgroup of order n in E (Fq) to protect against small subgroup attack [13].

Result – Verification and correctness

The protocol works correctly for the session can be shown as follows

For A

$$
\begin{aligned}
SK &= h\ (r_A.KU_B + M_B)\\
&= h\ (r_A.KU_B + r_B.KU_A)\\
&= h\ (r_A.KR_B.G + r_B.KU_A.G)\\
&= h\ (r_A.KR_B + r_B\ .KR_A).G\\
&= h\ (r_B.KR_A + R_A.KR_B).G\\
&= \text{Which is the SK of B.}
\end{aligned}
$$

For B

$$
\begin{aligned}
SK &= h\ (r_B.KU_A + M_A)\\
&= h\ (r_B.KU_A + r_A.KU_B)\\
&= h\ (r_B.KR_A.G + r_A.KU_B.G)\\
&= h\ (r_B.KR_A + r_A.KR_B).G\\
&= h\ (r_A.KR_B + r.KRA).G\\
&= \text{Which is the SK of A.}
\end{aligned}
$$

For the verification and for the Prof. of correctness we have to prove that r = r' so that its correctness can be prove as the same message received by the receiver send by the sender. In the verifying step.

$$
\begin{aligned}
r' &= [(g^{v1}\ Y_A{}^{v2})\ \mathrm{mod}\ p]\ \mathrm{mod}\ q\\
&= (g^{H(M)\ w\ \mathrm{mod}\ q}\ Y_A{}^{r\,w\ \mathrm{mod}\ q}\ \mathrm{mod}\ p)\ \mathrm{mod}\ q\\
&= (g^{H(M)\ w\ \mathrm{mod}\ q}\ g^{X_A\ r\ w\ \mathrm{mod}\ q}\ \mathrm{mod}\ p)\ \mathrm{mod}\ q)\\
&= (g^{H(M)\ w + X_A\ r\ w\ \mathrm{mod}\ q}\ \mathrm{mod}\ p)\ \mathrm{mod}\ q\\
&= (g^{(H(M)\ +\ X_A)\ w\ \mathrm{mod}\ q}\ \mathrm{mod}\ p)\ \mathrm{mod}\ q\\
\\
&= (g^{(((H(M)\ + X_A\ r)\ k\ H(M)\ +\ X_A\ r)\ -1\ \mathrm{mod}\ q}\ \mathrm{mod}\ p)\ \mathrm{mod}\ q\\
&= (\ g^{k}\ \mathrm{mod}\ p.)\ \mathrm{mod}\ q\\
&= r
\end{aligned}
$$

This correctness provides the authentication to the sender and receiver that a message which is signed is intended for the appropriate users [14].

In this paper we provide some further cryptography and analysis on the Phan's integration of DSA and Diffie-Hellman Key exchange protocol. We present an improvement on protocol with the help of two randomly selected integers which makes the protocol more secure [16[. Also these random numbers can provide two basic attributes for key exchange protocol i.e. - the forward secrecy as we have chosen the different random number each and every time as X_A and X_B which are private to both of users; Key Freshness as the public key of both user does not depend on each other it depends on the randomly selected value by users so key freshness can be maintained i.e. with the help of these random numbers we can generate a new key for every communication.

CONCLUSION

The research article provides insight cryptography on the basis of Phan's integration of DSA and DIffie- Hellman Key exchange protocol. This paper shows an improvement on protocol with the help of two integers selected randomly. This makes the protocol more secure. Randomly selected numbers equipped with two important attributes - The forward secrecy as chosen the different random number each and every time as X_A and X_B which are private to both of users; Key Freshness as the public key of both user does not depend on each other it depends on the randomly selected value by users so key freshness can be maintained i.e. with the help of these random numbers we can generate a new key for every communication.

Further, a new agreement protocol has been introduced based on the key confirmation. The protocol is developed that provides the utmost security attributes. These security attributes were never discussed in other key agreement protocols. The proposed security analysis of protocol against various types of attacks has further been equipped.

References

1. A. Arazi, \Integrating a key cryptosystem into the digital signature standard," Electronic Letters, vol.29, pp. 966-967, Nov. 1993.
2. W. Diffie and M. Hellman, "New directions in cryptography", IEEE Transactions on Information Theory, Vol. IT-l 22, No.6, November,1976, PP.644-654.
3. L. Harn, Ma. Mehta, and W. J. Hsin, \Integrating di±e-hellman key exchange into the digital signa-ture algorithm (DSA)," *IEEE Communication Letters*, vol. 8, no. 3, Mar. 2004.
4. Rescorla, E., Diffie-Hellman Key Agreement Method, RFC 2631, IETF Network Working Group, http://www.ietf.org/rfc/rfc2631.txt
5. R. C. W. Phan, \Fixing the integrated di±e-hellman-DSA key exchange protocol," *IEEE Communication Letters*, vol. 9, no. 6, Jun. 2005.
6. Curry, Ian, Entrust Technologies, "Getting Acquainted With Entrust/Solo and Public-key
7. Charanjit S. Jutla and Anindya C. Patthak. Is SHA-1 conceptually sound? Cryptology ePrint Archive, Report 2005/350, 2005. http://eprint.iacr.org/.

8. N. Howgrave-Graham and N. Smart, \Lattice attacks on digital signa- ture schemes", Designs, Codes and Cryptography, 23 (2001), 283-290.
9. Shafiqul Abidin, “Encryption and Database Security” *International Journal of Computer Engineering & Applications*, Vol XI, Issue VIII, (2321-3469), August, 2017.
10. M. Matsumoto and T. Nishimura, "Weight discrepancy tests on M-sequences", Bulltin of Yamagata University (Natural Science), Vol. 16, No.3, 2007, 105-112.
11. Bon Wook Koo, Hwan Seok Jang and Jung Hwan Song, Constructing and Crypt-analysis of a 16 £ 16 Binary Matrix as a Di®usion Layer. In K. Chae and M. Yung (Eds.): WISA 2003, LNCS 2908, pp.489-503, Springer-Verlag 2004.
12. “Cryptography and network security” by William Stalling Fourth edition.
13. Improved Authentication and Key Agreement Protocol Using Elliptic Curve Cryptography A. Chandrasekar, V.R. Rajasekar
14. NIST, "Special Publication 800-57: Recommendation for Key Management. Part 1: GeneralGuideline", Draft Jan.2003.
15. Shafiqul Abidin, Rajeev Kumar, A. R. Tripathy and Kumar Balwant Singh “ An Approach to Cryptosystem through a Proposed and Secured Protocol, *International Journal of Computer Applications* (0975 - 8887) Volume 50 - No.16, July 2012

How to cite this article:

Shafiqul Abidin (2017) 'Key Agreement Protocols & Digital Signature Algorithm', *International Journal of Current Advanced Research,* 06(08), pp. 5359-5362. DOI: http://dx.doi.org/10.24327/ijcar.2017.5362.0706

****