إخفاء الهوية بمخطط غرفة الصلاحية

Identity hiding by Authority Room scheme

المدرس الدكتور

صلاح عبد الهادي البيرماني

الكلية الاسلامية الجامعة – النجف الأشرف

اخفاء الهوية بمخطط غرفة الصلاحية

Identity hiding by Authority Room scheme

المدرس الدكتور

صلاح عبد الهادي البيرماني

الكلية الاسلامية الجامعة – النجف الأشرف

Abstract:

In this paper we use public key cryptosystems to keep the message by hiding the identity of the Customer's public key by pseudo key from Room of trust worthy. The key center generated from two public keys in the Room of Distribution Center. The Public key use to encryption and the private key for decryption of Ciphertext, the secretary is signing the message sent by the customer blindly without learn any think about the Customer and the message by check the validity of the Customer from the server of the database.

By sending the Ciphertext through multiple Authority Rooms (group of users authentications) without breaking the public key of the message because its transfer blindly through the Authority Room after check the validity of the sender ID and its Authority Room ID_R.

Each Authority Room has two keys, public key of the previous Authority Room (to recover the Ciphertext) and its own private key (for signing the Ciphertext) then resend the signing message to the next Authority Room.

This method is fit to multiple Customers, Managers and for multiple Authority Rooms to transfer the message from the sender to the receiver and encrypted the message by receiver

public key hiding and blindly signing after transfer through multiple Authority Rooms, in this paper we used RSA algorithm for encryption and signing process.

Keywords

Cryptography, Cryptosystem, Public key, blind Signature, Digital Signature. DSS، Authentication, Authority Room.

I. Introduction

In this paper will utilize the public key systems for group of users using the Authority Room signature and blind signature to hide the identity of the Customer through multiple Authority Rooms without key breaking their definition will be presented in section 3 will be about the mechanism of protecting the information by using Authority Rooms.

Public key cryptography was invented in 1976 by Whitfield Diffie and Martin Hellman [1] . it is sometime called Diffie-Hellman encryption. It is also called asymmetric encryption because it uses two keys instead of one key (symmetric encryption).

The implementation of this Algorithm for security is illustrated in figure 1 for a plain message M to be sent from sender A to receiver B , it is encrypted using the receiver's public key KU_b to get Ciphertext C as

$$C = E_{KU_b}(M) \qquad (1)$$

While at the receiver,it is recovered by a decryption process using the private key KR_b as

$$D_{KR_b}(C) \Rightarrow M \qquad (2)$$

Therefore, this message can only be recovered by the person who has the private key.

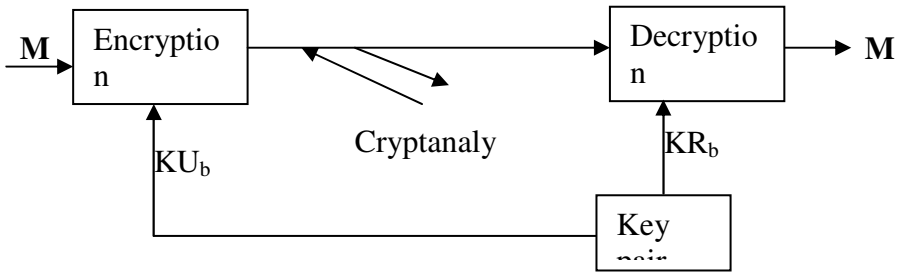

Fig 1. the public key Cryptosystem for security.

I.I RSA Algorithm

In cryptography, RSA is an Algorithm for public-key cryptography. It was the first Algorithm known to be suitable for signing as well as encryption, and one of the first great advances in public key cryptography. RSA is widely used in electronic commerce protocols, and is believed to be secure given sufficiently long keys and the use of up-to-date implementations[1][2].

This Algorithm was publicly described in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman at MIT, the letters RSA are the initials of their surnames. [4],[5],[6]

RSA involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key. The keys for the RSA Algorithm are generated the following way:

1. Choose two distinct large random prime numbers p and q
2. Compute n=pq
   n is used as the modulus for both the public and private keys
3. Compute totient: the $\phi(n) = (p-1)(q-1)$.
4. Choose an integer e such that $1 < e < \phi(n)$, and $\phi(n)$ share no factors other than 1 (i.e. e and $\phi(n)$ are coprime)
   e is released as the public key exponent
5. Compute d to satisfy the congruence relation $de = 1 \pmod{\phi(n)}$; i.e. $de = 1 + k\phi(n)$ for some integer k.
   d is kept as the private key exponent

Encrypting messages

B transmits his public key (n,e) to A and keeps the private key secret. A then wishes to send message M to B.

He first turns M into a number m<n by using an agreed-upon reversible protocol known as a padding scheme. He then computes the Ciphertext C corresponding to:

$$C = m^e \bmod (n) \qquad (3)$$

This can be done quickly using the method of exponentiation by squaring. A then transmits to B.

Decrypting messages

Alice can recover m from c by using her private key exponent d by the following computation:

$$m = c^d \bmod (n) \qquad (4)$$

Given m, he can recover the original message M.

2.2 RSA scheme

To sign the message m , first the private key of the sender is used to calculate a Ciphertext called signature S

$$S = D(m) = (m)^d \bmod (n) \qquad (5)$$

This cryptogram is transmitted over the insecure channel. Any one can use the public key of the sender can recover the message m by performing the inverse of equation (5)

EA (S) =(S)e mod (n) ==> m' (6)

If m' = m then the message is authentic and are sure that the message has been sent by user who claims to be the sender and this is the main idea of this paper by using the Authority Room for singing the Ciphertext and resend it through unsecured network.

2. Authority Rooms

In this paper we used meaning of Authority Room to increase the security of information and decisions during the administration levels in the organization without change or effect on the type of administration's connections. Each Authority Room is connected to another Room during chain of commands; in the electronic system the Authority represent the power or the ability to do actions[7].

The Authority Room is the home of decision represented by single user , single group or multiple groups, and each Room could have multiple authentications also the Authority Room can't exist in the electronic organization unless there is at least one user, and each user want to enter the Authority Room should have the permission which is different from Room to another and this is the responsibility of the administrator who is also responsible for security of information[8] , method of encryption, making decisions and key distribution in order to perform the Authentication, Authorization and Auditing.

The Authority Room is an object that has properties like independency, hiding information and we can use processing procedures by using programming methods.

The Authority Rooms can contact each authors by using protocols (set of rules that govern the data communication) like messaging protocols and parameters which describe the situations of the Authority Room before and after receiving the messages see Fig 2.

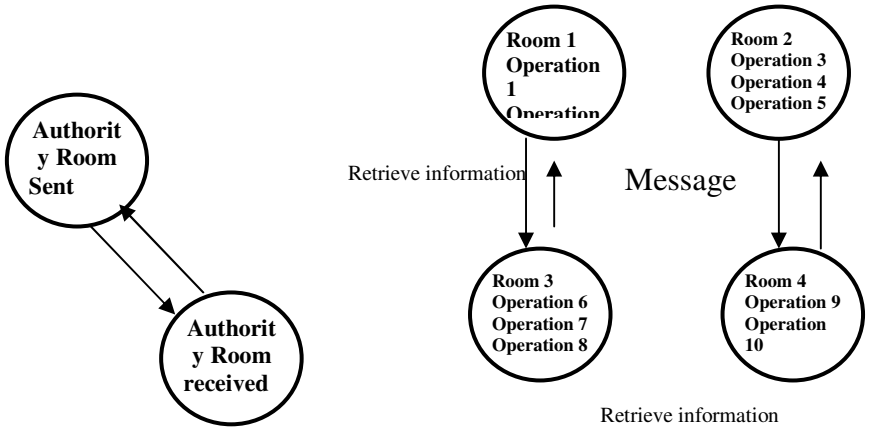

Fig 2 Transferring information and Messages between Authority

There are several methods of key distribution in the Authority Room systems like the following

- Suppose that we have (n) Authority Rooms that are connected together from upper to lower, the first Room represent the root of the decision and the last Room represent the tail of the decision and each Room has connected to the server of the Data Base to get its own public key of the message of the decision Root Room for Authentication.

- And we can distribute different keys to the Authority Rooms' tree, the first Room get K1 and the second Room get K2 and so on until Room (n-1) which get Kn-1 ,
- The message is encrypted by decision Root Authority Room:--

$$C=f(M, K); \quad (7)$$

As C represent cryptogram of a message M which is encrypted by the key K.

The first Authority Room decrypts the crypto message by key K1 then encrypts the crypto message C by key X1:

$$M=g(C, K1); \quad (8)$$

$$C1=f(C, X1); \quad (9)$$

Then the first Authority Room sends the C1 to the second Authority Room which decrypts a message C1 by key K2 and encrypts the crypto message by key X2 by the same way C2 is sent to the third Authority Room and so on until the Authority Room that represent the decision tail.

Each Authority Room should send its own public key to the other Authority Rooms but still the Authority Room in the bottom can't send to the top Authority Room without permission

There are three factors should be available to protect the data which are the administration of the organization[9], the type and structure of the electronic networks and the data protection methods[10].

3. The proposed Authority Room scheme

3.1 Identity hiding

In this paper we suggested a method suitable for group of Customers communication with group of Managers by using the Authority Room scheme to hide the identity of the Customers by using the public key generated blindly from the Managers and

third person we call him the secretary and by using the Authority Room to sign the message blindly after checking the authentication of Customer and his Authority Room, by this way we can send the Ciphertext through infinite nodes (Authority Rooms) by using any Algorithm and with using a hidden key.

Each Authority Room had secretary who responsible for the database confidentiality and to sign the document blindly then sends it to the Manager or to next Authority Room .

The method can be summarized as follows:

In the Authority Room who represents the tail of the decision, each Manager generates two keys, one private he keeps for himself and one is public , he gives it to the distribution center Authority Room e.g. Manager 1 generates d_{M1} and e_{M1} respectively, more over a secritory generates two respective keys d_S and e_S too. This center will generate a general key K_{G1} as e_{M1} e_S. this key is then sent to trustworthy center Authority Room , who will be made public.

And Customer at any Authority Room can encrypt a document M with key K_{G1} getting the Cryptogram C after he signed it by his private key as:

$$C = E_{kG1}(E) \quad (10)$$

Where

$$E = D_{dc}(M) \quad (11)$$

Then C is signed by the Customer's Authority Room and then sent it to the next Authority Room with the Customer's ID and his Authority Room's ID_R as:

$$S_M = f(C,K) \quad (12)$$

The secretary at each Authority Room check the validity of the both ID_S by directly consulting the database, After the C is

received by the secretary who sent his public key he will sign the message by his own private key and sent it to the Manager who used his private key also to decrypt the received signed cryptogram, which will reveal the original clear message M as:

$$C = g(S_M, X) \quad (13)$$

$$D_{dM1}(S) = D_{dM1}(D_{KS}(C)) \quad (14)$$

$$D_{dM1}(S) = D_{dM1}(D_{KS}(E_{KG1}(M))) \quad (15)$$

Fig 3 illustrates the whole security scheme.

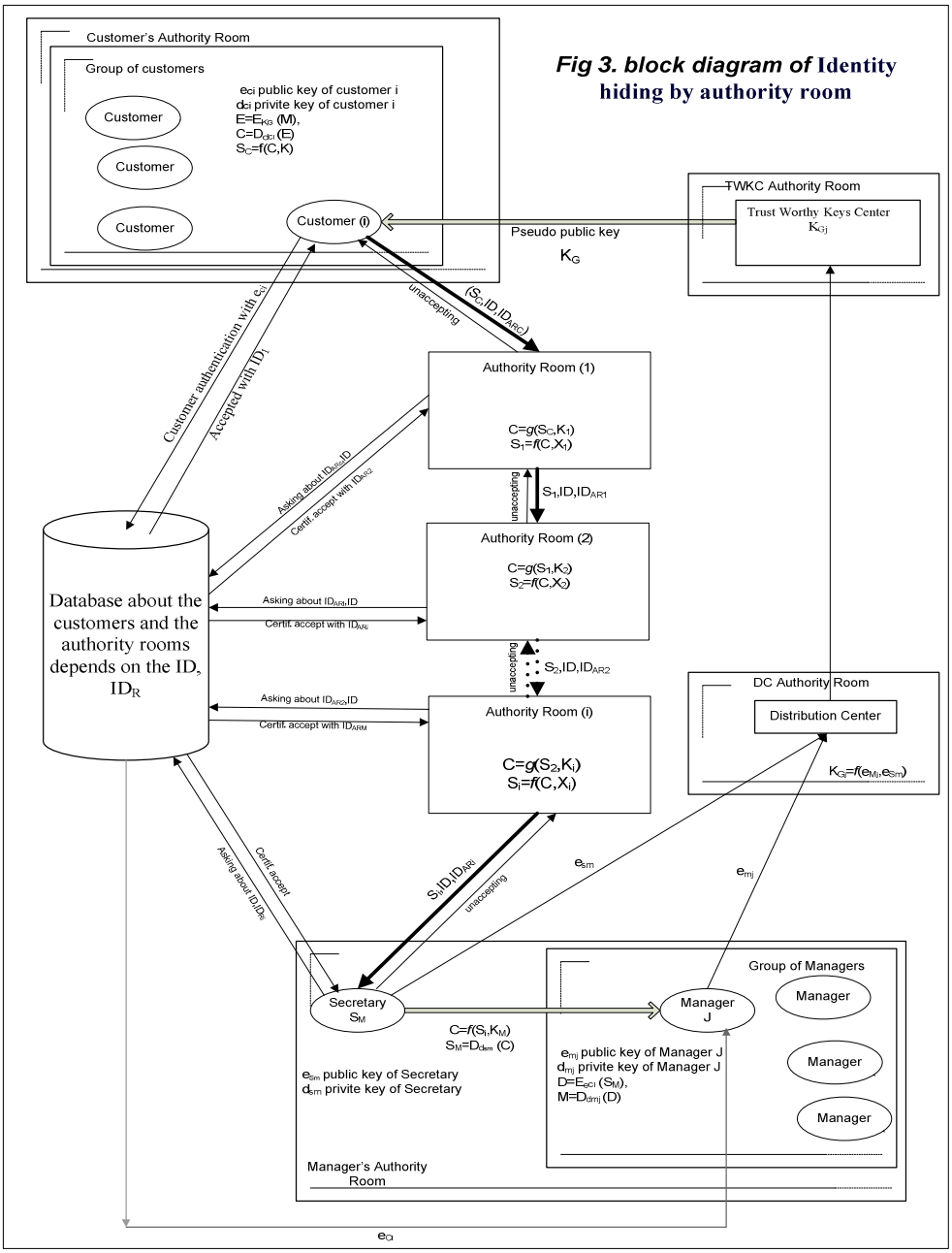

Fig 3. Identity hiding by Authority Room scheme

3.2 The Algorithm

Let us follow RSA Cryptosystem to illustrate the Algorithm for the suggested identity hiding by using Authority Room scheme.

Two large prome p&q are chosen, then their product N is calculated as N=pq.

Let N =(p-1)(q-1) and E&D are encryption and decryption Algorithms respectively . for the secretary two keys e_{sm} &d_{sm} are selected such that

e_s d_s mod ϕ(N) =1. also for each Manager j two keys are selected e_{Mj} &d_{Mj} such that e_{Mj} d_{Mj} modϕ(N) =1. then d's are kept private and e's are sent to a DC Authority Room this Center calculate new general key for each Manager by $K_{Gj} = e_{sm}$ e_{Mj} these keys are sent to the TWKC Authority Room and will be used for encryption over the communication network.

The Algorithm proceeds as follows:

At the Customers Authority Room: any Customer like to send a message M to the Manager j in the Manager's Authority Room he encrypts his message as

$$C = M^{KGj} \bmod N = M^{eseMj} \bmod N \qquad (16)$$

The Customer sign the message M by his private key and the Authority v Room sign the Ciphertext C by its private key as

$$S_C = C^K \bmod N = C^{dARC} \bmod N \qquad (17)$$

Then the Customer sends his ID and his public key e_{ci} to the database server to take the order for accept or reject the message and the server sends to the Customer the ID of the next Authority Room (could be the Manager's Authority Room or deferent Authority Room will be in the middle of the process), then he sends his ID,ID_{AR} and his signed message to the secretary of the next Authority Room.

At the Authority Room: if the Customer ID and Customer's Authority Room accepted , the Authority Room (1) will recover the Ciphertext C and then signs by its own private key and then resend it to the next Authority Room as

$$C = g(SC, K1) = S_C^{esc} \bmod N \quad (18)$$

$$S1 = f(C, X1) = C^{ds1} \bmod N \quad (19)$$

And all the Authority Rooms follow this role.

At the secretary: after checking the validities of the Customer and the Authority Rooms , The secretary signs the cipher message by private key d_{sm}

$$SM = D_{dsm}(C) = C^{dsm} \bmod N = M^{esm\ eMj\ dsm} \bmod N \quad (20)$$

$$==> M^{eMj} \bmod N$$

At the Manager: finally , the Manager will use his private key dMj and the Customer's public key to recover the original message M as

$$S^{dMj} \bmod N = (M^{eMj} \bmod N)d^{Mj} \bmod N$$

$$= (M)^{eMjdMj} \bmod (N) ==> M \quad (21)$$

The whole process is shown in fig 4

AR : The Authority Room
Cust (i) : The Customer i.
Manag (j) : The Manager j.
Secr ( ) : The Secretary( )

DBC : Database about the Customers to given Certificate
DC : Distribution Center
TWKC : trust worthy keys center

Send (S, R, a, b, ..) : Method to send a, b, ... from the sender S to receiver R
Access (C, S, a, b, ..) : Method access the client C to Server S to asking about a, b, ...
I D : The Identification of

Initialization {
Send (Manag (J), DC, e_{mj});
Send (Secr(S_M) , DC , e_{sm});
DC: KG = f (e_{mj}, e_{sm});
}
Customer i {
Access (Cust(i),TWKC,KG);
E = E_{KG} (M);
D = D_{dci} (E);
S_c = *f* (C,K);
Send (Cust (i), DBC, ID, $ID_{AR(C)}$, e_{ci}, cetif);
Send (DBC , cust (i) , Customer authentication, $ID_{AR(1)}$);
Send (Cust (i), Secr(S_1), S_c,ID,$ID_{AR(c)}$);
}
Authority Room (1) {
Access (Secr(S_1), DBC, certif.);
Send (DBC, Secr(S_1),certif., $ID_{AR(2)}$);

If (certif. = = false){
Send (Secr(S_1), Cust (i), unaccepting);
STOP;
}
else {
Secrt (S_1): C = g(S_c,K1);
S_1 = f(C,X1);
Send (Secr (S_1),Secr(S_2), S_1, ID,$ID_{AR(1)}$);
}
}
Authority Room (2) {
Access (Secr(S_2), DBC, certif.);
Send (DBC, Secr(S_2),certif., $ID_{AR(i)}$);
If (certif. = = false){
Send (Secr (S_2), Secr (S_1),unaccepting);
STOP;
}
else {
Secr (S_2): C = g(S1,K2);
S_2 = f(C,X2);
Send (Secr (S_2),Secr(i),S_2,ID,$ID_{AR(2)}$);
}
}

Authority Room (i) {
Access (Secr(S_i), DBC, certif.);
Send (DBC, Secr (S_i),certif., $ID_{AR(m)}$);
If (certif. = = false){
Send (Secr (S_i), Secr (S_2), unaccepting);
STOP;
}
else {
Secrt (S_i): C = g(S_2,Ki);

$S_i = f(C,Xi)$;
Send (Secr (S_i),Secr(S_M), S_i, ID,$ID_{AR(i)}$);
}
}
Authority Room (M) {
Access (Secr (S_M), DBC, certif.);
Send (DBC, Secr (S_M), certif.);
If (certif. = = false){
Send (Secr (S_M), Secr (S_i), unaccepting);
STOP;
}
else {
Secr (SM): $C = g(S_i,KM)$;
$S_M = D_{dsm}(C)$;
Send (Secr (S_M),Manag(J), S_M);
}
Manag (J){
$D = E_{eci}(S_M)$;
$M = D_{dmj}(D)$;
}
}

Fig 4. The Algorithm for Identity hiding by Authority Room scheme

6. Implementation

The suggested algorithm in sections 3 & 4 is practically implemented using RSA technique. The program is written in Java Sun language in NetBeans program. The two prime numbers p & q were chosen of 50 digits length each, the public keys for the manager and secretary at the Manager's Authority Room (emj & esm) , public key of the customer(eci),public key

of secretary of customer's Authority Room (psarc),public key of secretary of Authority Room 1 (psar1), public key of secretary of Authority Room 2 (psar2) and public key of secretary of Authority Room i (psari) are of 90 digits length, respectively. The private keys of all the public keys were calculated. Then a message, M of 95 digits length is encrypted using the general key kG and signed by the private keys of the customer and his room, then sent together with the customer's ID to next Authority Room as Sc and so on. At the manager's authority room the secretary signed the message after checking the validity and sent to the manager. The manager, using his or her private key recovers the original message. An example showing the steps for actual keys and message encryption, signing, validation and message recovery is shown in bellow; the message block length is taken of the order of 50 digits.

P=
22953686867719691230002707821868552601124472329079(50 digit)

q=
30762542250301270692051460539586166927291732754961(50 digit)

All public Keys are (90digit).

The public key of the Manager in the Manager's Authority Room (emj):
35752334942676003169313626814655695963315290125751655287486460091602385142405742365191277

The private key of the Manager in the Manager's Authority Room (dmj):
79304729128845707084524237256483902478378090450919845313366991538561845340970578567647258729357573

The public key of the Secretary in the Manager's Authority Room(esm):
37463219851875188754857455984529384564398469216501266754813821619984472224780876757777279

The private key of the Secretary in the Manager's Authority Room(dsm):
25215822705303211453668684214355988551411899933629211465812130798311239453454778275938466787877599 9

The public key of the Customer in the customer's Authority Room(eci):
20400572826609004877725320724141666905147636921650126675481382161998447222478087648834427 9

The private key of the Customer in the customer's Authority Room (dci):
26892319319452146567552740828886107820705641856976802845633902141785389782630549560355151681222579 9

The general key kG= emj esm mod (ø(N)):
25618853736714909843116961944720268313514536063361797739350376077324607187046729285790987319219880 3

The public key of the customer's Authority Room(psarc):
90400572826609004877725320724141666905147636921650126675481382161998447222478087648839753 1

The private key of the customer's Authority Room(dsarc):
70405131408220387179653058277975443537808048701219008634733737151320991483725270128346195975419301 1

The public key of the Authority Room (1)(psar1):
50400572826609004877725320724141666905147636921650126675481382161998447222478087648834427 9

The private key of the Authority Room (1)(dsar1):

132728089937190947903330695012110624463146278782449190048140729608959168054876901006587208857108519

The public key of the Authority Room (2)psar2):

138986709828713303267526583073316669051476369216501266777813821619984472224780876488386597

The public key of the Authority Room (2)(dsar2):

927448872199890706309261043199477320024971417864187041659682007874531099643062989102536160168814 53

The public key of the Authority Room (i)(psari):

579152334942676003111313626814655695963315290125751655287486460091602385142405742365191209

The public key of the Authority Room (i)(dsari):

503698435867397796875970604927110057193483319293903493639147521048360019339523772371401091103362809

the Message

M=764652387562347625883476523049809852349751243987507821695212210760858748099647472111729127512992589912196684750549658310084416732550077367495770217142995264954367409534876309875603496857304895673459862(200 digit),(the block=50)

At the customer room ,he encrypt the message m with Kg and sign it with his private key (dci) and his room's private key(dsarc)

Sc=754254667903383790644044027316873076730425895630859364576532700903031118840831398873459404766821678908919825346787416493967429668326829003898710004433128357845067713474337811893339198358785509459935171302953046149897380466539421354878866975824041049640163350173555247899650107485030261948319751742000118766569008214185876483057941658327281555812541732925770635956358158273442802 93

at the Authority Room (1) the secretary unsigned the Message Sc by customer Authority Room's public key and sign it by his private key

S1=514299451992249486468450229721760847360355931867187843930271742569121580774839778984170603770416567605869884504056442060904143889459118967860340292114953924647774104657143576252376407330014799343235546584711780068320309758035580588365487048223645714690242332043803999859665077068714185748135493244463658423880709831864695703047729181499944452944824740069496260037664510612824392741786152180934118

at the Authority Room (2) the secretary unsigned the Message S1 by first Authority Room's public key and sign it by his private key

S2=
511227675657252014904316676710898864357202224562940836436739746580780043630436591402942413436200360312205676033057545780865000536034844038523624773788338458205310618664230842603577619533263093391394438583543523573984051766283684754161986378175968143592610717932259350734202220177691328930751165683571335704467495338648410910323000407382495839353365174204851581594647952755201051340996392306974443

at the Authority Room (i) the secretary unsigned the Message S2 by second Authority Room's public key and sign it by his private key

Si=
633443403524956740838391466696393786130777787241977893595213897160020440005601059820636776959373615590274808715529781726814006988059327735787468788595637584336404061856040616089529309399635021657138677942442732497166376633877271339969819489093106467500067361469787157899644993065774389920941087849980082148471531

468565090577241901240523914523079644431346638648860102319155770483229022750859951 9

at the Manager's Authority Room the secretary unsigned the Message Si by i Authority Room's public key

Sm=

619758054291450790644307663638491168645859525483337662875223827209422501980974998422951909304287988611092097597845558842640346299720049468737762347061403696205261951786135733134945238255937529424818430995738837404901699478811177580567437857955528618207168620437135968500926110557091924048067671388474644484600112321836253771047276825295947621175759868611090964133501865142744634373679289577062 06

At the Manger's Authority Room the Secretary blindly sign the Message Sm by his private key dsm

C=

493667077613896130102961735751865252567168582055752045518118995058152673038189384349430550463795440579438816449123772068466732360510038698465155501750619393007372996460092240437707469732505616519198402075263264972651628143478362301205172098746720892748761832664376156523414003689888201904316572008304848077389445404043376897048115894794248387877417445770908780922883893361579473706675205851133348

At the Manger's Authority Room the Manager unsigned the Message C by the Customer's public key eci and decrypt it by his private key dmj

M'=

764652387562347625883476523049809852349751243987507821695212210760858748099647472111729127512992589912 19

668475054965831008441673255007736749577021714299526495436740953487630987560349685730489567345986

==> M

6. Conclusion

A new generalized identity hiding by blind signature in Authority Room is presented, by using this new term (Authority Room), any group of users or Customers can communicate with any group of Managers are located in another Authority Room directly or by using N Authority Rooms in the middle of communication if the Customers and the Managers Authority Rooms didn't have directly contact. Each Authority Room can't learn the message or the any information about the sender and signed the message blindly ,this kind of communication has advantages and wide applications in many fields.

The advantages

- The sender will not be able to know the public key (Cryptographer) for the intended receiver (Manager).
- Each of the receiver (Manager) and secretary in the Manager's Authority Room can change their public key individually and this process does not follow any specific rules.
- In this method, there are both signature and encryption inside the same message.
- The public keys used by any organization are pseudo keys, which do not give any information about the key.
- Each Authority Room signed the Ciphertext without learn on the message or the identity of the sender.

- If the sender Authority Room has no directly contact with the receiver Authority Room, he can use N Authority Rooms in the middle of communication.
- Any Algorithm can use it in this communication's scheme.

And the applications

- By using banks agreements the Customer can deposit money from any bank inside this agreement by using the web-site, so that all information related to the money and other details will be encrypted under the key KG which is obtained from a trustworthy data base whose function is providing keys along with account numbers, considered as ID's and passwords used for login, when it is necessary for more documentation to the Customer ,so the bank who communicate with use the Authority Room scheme to communicate with your bank.
- Commercial companies dealing with permanent dealers and Customers having ID's within the sales and purchases services.
- Governmental organizations, especially those both with sensitive and confidential information, e.g. those related to national security, military, intelligence and other sensitive organizations.

7.References

[1] W. Diffie and M. Hellman, New directions in cryptography. IEEE Transactions on Information Theory IT-22, 644-654, 1976.

[2] R. Rivest, A. Shamir and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM 21, 120-126, 1978.

[3] I. Blake, G. Seroussi and N. Smart, Elliptic Curves in Cryptography. Cambridge University Press, Cambridge, 1999.

[4] Menezes, Alfred; van Oorschot, Paul C.; and Vanstone, Scott A. Handbook of Applied Cryptography. CRC Press, October 1996. ISBN 0-8493-8523-7

[5] R. Rivest, A. Shamir, L. Adleman. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM, Vol. 21 (2), pp.120–126. 1978. Previously released as an MIT "Technical Memo" in April 1977. Initial publication of the RSA scheme.

[6] Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, and Clifford Stein. Introduction to Algorithms, Second Edition. MIT Press and McGraw-Hill, 2001. ISBN 0-262-03293-7. Section 31.7: The RSA public-key cryptosystem, pp.881–887.

[7] Pringle, Charles D., et. Al., (1988), "Management Organizations: function and behaviors Colums:", Merrill Publishing Company.

[8] Tosi, Henry I.,et.A1,, (1986), "Managing Organizational behavior", Cambridge: bellinger publishing Company.

[9] Richard J. Staron, (2001), "Networking Complete", SYBEX, ISBN:0-7821-2968-4.