A STUDY ON KEY ESTABLISHMENT

A Dissertation submitted in partial fulfillment of the

Requirement for the award of

DEGREE OF MASTER OF SCIENCE

IN MATHEMATICS

By

MARIA ALEENA ANTONY

REGISTER NO: SM16MAT008

(2016 – 2018)

DEPARTMENT OF MATHEMATICS

ST.TERESA'S COLLEGE, (AUTONOMOUS)

ERNAKULAM, KOCHI - 682011

APRIL 2018

DEPARTMENT OF MATHEMATICS

ST.TERESA'S COLLEGE (AUTONOMOUS), ERNAKULAM

CERTIFICATE

This is to certify that the dissertationentitled "A STUDY ON KEY ESTABLISHMENT" is a bonafide record of the work done by MARIA ALEENA ANTONY under my guidance as partial fulfillment of the award of the degree of Master of Science in Mathematics at St.Teresa's College (Autonomous), Ernakulam affiliated to Mahatma Gandhi University, Kottayam. No part of this work has been submitted for any other degree elsewhere.

ALKA BENNY (Supervisor)

Assistant Professor

Department Of Mathematics

St.Teresa's College,(Autonomous)

Ernakulam

Smt Teresa Felitia (HOD)

Associate Professor

Department of Mathematics

St. Teresa's College (Autonomous)

Ernakulam

External Examiners:

1. ..... **2. .....**

DECLARATION

I hereby declare that the work presented in this project is based on the original work done by me under the guidance of ALKA. BENNY, Assistant Professor, Department of Mathematics, St Teresa's College (Autonomous) Ernakulam and has not been included in any other project submitted previously for the award of any degree.

ERNAKULAM

APRIL 2018

MARIA ALEENA ANTONY

REGISTER NO: SM16MAT008

ACKNOWLEDGEMENT

I express my sincere gratitude to my guide Ms.Alka Benny, Assistant Professor, Department of Mathematics, St.Teresas College, Ernakulam , for helping me in the successful completion of this work.

I further express my gratitude to Smt.Teresa Felitia, Head of department of Mathematics, St.Teresas College, Ernakulam and other teachers of the Department for their encouragement, suggestions and assistance in taking up this dissertion.

I finally thank my parents, friends and all my well wishers who supported me during the preparation of this project. I bow my head before God almighty without whose blessings i wouldn't be able to complete this work.

ERNAKULAM

APRIL 2018

MARIA ALEENA ANTONY

REGISTER NO: SM16MAT008

CONTENTS

INTRODUCTION

Cryptography is concerned with the study of secure protocol design.Key establishment protocols are procedures to derive a shared secret key by two or more parties over an openly distributed networks.These protocols are important building blocks in cryptography,and in particular,are fundamentally required to build secure communications channels over insecure channels.

There are two major techniques of key establishment,key transport and key agreement.we assume that a public key infrastructure is in place,which may or may not be used by the key establishment protocols.There have been numerous proposal for key establishment protocol,but unfortunately many of them are vulnerable to un anticipated security problems.

In this project we examine security models and key establishment protocols.We begin with key agreement.This section presents key agreement protocols based on symmetric techniques and key agreement based on asymmetric techniques.Next section we discuss about the key transport.Here also we have two sub sections they are key transport based on symmetric encryption and key transport based on public key encryption .Then we discuss about the cryptographic key life cycle.The set of stages through which a key progress during its existence.

PRELIMINARY

Key management plays a fundamental role in cryptography. As the basis for securing cryptographic techniques providing confidentiality,entity authentication,data origin authentication,data integrity and digital signatures.The goal of a good cryptographic design is to reduce more complex problems to the proper management and safe keeping of a small number of cryptographic keys.

In real time keying relationships in a communications environment involve atleast two parties (a sender and a receiver).In a storage environment there may be only a single party,which stores and retrieves data at distinct points in time.
The objective of key management is to maintain keying relationships and keying material in a manner which counters relevant threats

•Compromise of confidentiality of secret keys.

•Compromise of authenticity of secret or public keys.Authenticity requirements include knowledge or verifiability of the true identity of the party a key i shared or associated with.

•Unauthorized use of secret or public keys

KEYING RELATIONSHIP

A Keying relationship is the state wherein communicating entities share common data (keying materials) to facilitate cryptographic techniques.

PROTOCOL

A Protocol is a multi-party algorithm,defined by a sequence of steps precisely specifying the actions required of two or more parties in order to achieve a specified objective.

KEY ESTABLISHMENT

Key establishment is a process or protocol whereby a shared secret becomes available to two or more parties for subsequent cryptographic use.It can be divided into Key Transport or Key Distribution and Key Agreement.
A key transport protocol or mechanism whereby one party chooses a secret

key or keys and then transmits them to another party or parties in encrypted form.
key agreement denotes a protocol whereby two(or more parties) jointly establish a secret key by communicating over a public channel.

KEYS

There are two types of keys
∗long-lived keys (LL Keys)
∗Short lived session keys

Long-Lived Keys

Users (or pairs of users) may have Long-Lived Keys which are precomputed and then stored securely.Alternatively LL Keys might be computed non interactively as needed from securely stored secret information LL Keys could be secret keys known to a pair of users or to a user and trusted authority.

Short-Lived Session Keys

Pair of users will often employ secret Short Lived Session keys in a particular session and then throw them away when the session has ended.
Session keys are useful
•They limit the amount of cipher text available to attacker because session keys are changed on regular basis.
•They limit exposure in the event of session key compromise.
•Reduce the amount of long term storage of a large number of distinct secret keys,by creating keys only when actually required.
•Also session keys are used to create independence across communications sessions or applications.

Key Predistribution scheme

Key predistribution scheme provides one method to distribute secret LL keys ahead of time.It requires a secure channel between the trusted authority and each network user at the time that the keys are distributed.

Passive Attack

A passive attack involves an adversary who attempts to defeat a cryptographic technique by simply recording data and thereafter analysing it.

Active Attack

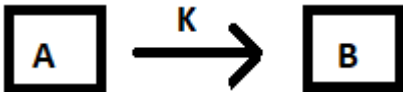
An Active attack involves an adversary who modifies or injects messages.

SIMPLE KEY ESTABLISHMENT MODELS

Here simple implies involving atmost one 3^{rd} party.

K_{XY}-symmetric key shared dy X and Y.

a) Point-to-point key distribution



These involve two parties communicating directly.

b) Key Distribution Center (KDC)

Fig 1

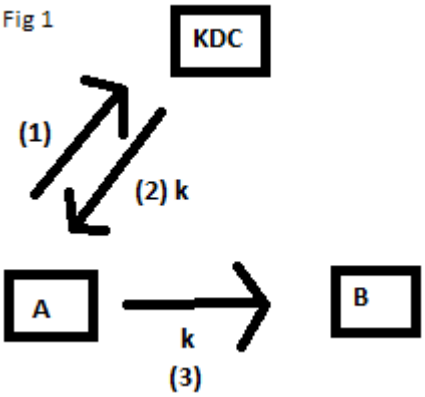
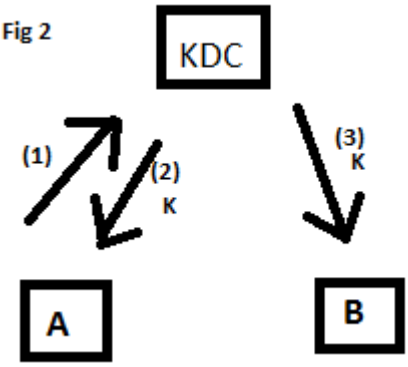


Fig 2



KDC are used to distribute keys between users which share distinct key with the KDC but not with each other.A basic KDC protocol,

Upon request from A to share a key with B.

The KDC T generates or otherwise acquires a key K,then sends it encrypted under K_{AT} to A,along with a copy of K(for B) encrypted under K_{BT}. Alternatively T may communicate k to B directly.

c) Key Translation Center (KTC)

Fig 1

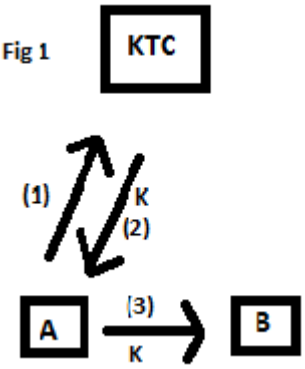
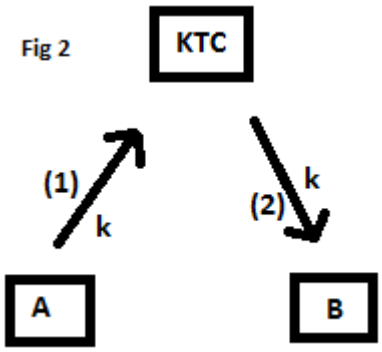


Fig 2



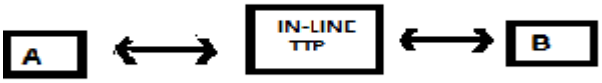
Same as KDC but her one of the parties supplies the session key rather than the trusted center. A basic KTC protocol: A sends a key K to KTC T encrypted under K_{AT}.The KTC deciphers and re-enciphers K under K_{BT},then returns this to A (to relay to B)or send it to B directly.

ROLE OF THIRD PARTY

From a communications viewpoint,three categories of third parties T can be distinguished based on relative location to and interaction with the communicating parties A and B.

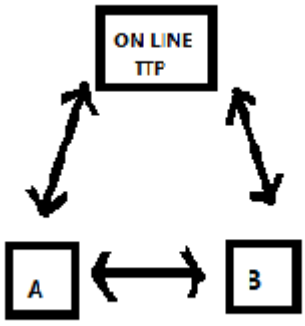
IN-LINE

T is an intermediary,serving as the real time means of communication between A and B .



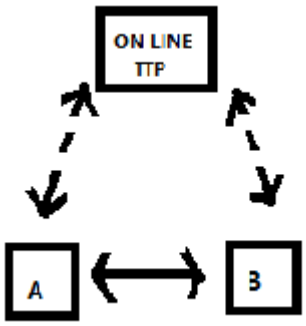
ON-LINE

Third party is involved in real time during each protocol instance (communicating with A or B or both) but A and B communicate directly rather than through third party.



OFF-LINE

Third party is not involved in the protocol in real time,but prepares information a priori,which is available to A or B or both and used during protocol execution.


ON LINE
TTP
A
B

CHAPTER 1

KEY AGREEMENT

1. KEY AGREEMENT BASED ON SYMMETRIC TECHNIQUES

1.1 The Blom Key Predistribution scheme

Assume that trusted authority(TA) distributes secret information securely to n network users.The adversary may corrupt a subset of atmost k users and obtain all their secret information,where k is a pre-specified security parameter.The adversary's goal is to determine the secret LL keys of a pair of uncorrupted users.The Blom key predistribution scheme is a KPS that is unconditionally secure against adversaries of this type.
It is desired that each pair of users U and V will be able to compute a key K_{UV}=K_{VU}.So any set of users other than U and V must be unable to determine any information about K_{UV}.
In the blom key predistribution scheme ,keys are chosen from a finite field Z_P ,where p≥n is prime.The TA will transmit k+1 elements of Z_P to each user over a secure channel.

The Blom key predistribution scheme has two cases
1) when k=1
2) for an arbitrary k.

First we present the Blom's scheme where k=1.
Here the TA will transmit two elements of Z_P to each user over a secure channel.
Protocol is given by
Blom KPS

STEP 1:A prime number p is made public and for each user U,an element $r_u \in Z_P$ is made public.The element r_u must be distinct.
STEP 2: The TA chooses three random elements a,b,c$\in z_p$ (not necessarily distinct) and forms the polynomial
f(x,y)=a+b(x+y)+cxy(mod p)
STEP 3: For each user U,the TA computes the polynomial

$g_u(x) = f(x, r_u)(modp)$
and transmits $g_u(x)$ to U over a secure channel.Note that $g_u(x)$ is a linear polynomial in x, so it can be written as

$g_{u(x)=a_u+b_u x}$
where $a_u = a + b_{r_u}(modp)$
$b_u = c_{r_u}(modp)$
STEP 4: If U and V want to communicate,then they use the common key
$k_{u,v} = k_{v,u} = f(r_u, r_v) = a + b(r_u + r_v) + cr_u r_v(modp)$
where U computes, $k_{u,v} + g_u(r_v)$ and V computes, $k_{v,u} = g_{v(r_u)}$
An important feature in the protocol is that the polynomial f is symmetric $f(x, y) = f(y, x)$ for all x,y.
This property ensures that$g_u(r_v) = g_v(r_u)$

EXAMPLE

suppose the three users are U,V and W,p=17 and their public elements are $r_u = 12, r_v = 7 and r_w = 1$.Suppose that the TA chooses a=8,b=7 and c=2 so the polynomial is
$f(x, y) = a + b(x + y) + cxy(modp)$
$ie, f(x, y) = 8 + 7(x + y) + 2xy(mod17)$
The g polynomial are given by
$g_u(x) = a_u + b_{ux}$
where $a_u = a + br_u(modp) \text{and} b_u = b + cr_u(modp)$

To find g_u

$a_u = a + br_u(modp)$
$= 8 + 7 \times 12(mod17)$
$= 7$
$b_u = b + cr_u(modp)$
$= 7 + 2 \times 12(modp)$
$= 14$
$\therefore g_u(x) = 7 + 14x$

To find$g_v(x)$

$a_v = a + br_v(modp)$
$= 8 + 7 \times 7$

$= 6$
$b_v = b + cr_v(modp)$
$= 7 + 2 \times 7(mod17)$
$= 4$
$\therefore g_v(x) = 6 + 4x$

To find g_w

$a_w = a + br_w(modp)$
$= 8 + 7 \times 1(mod17)$
$= 15$
$b_w = b + cr_w(modp)$
$= 7 + 2 \times 1(mod17)$
$= 9$
$\therefore g_w(x) = 15 + 9x$

$\therefore g_u(x) = 7 + 14x$
$g_v(x) = 6 + 4x$
$g_w(x) = 15 + 9x$

To get the Keys U compute:

$k_{u,v} = g_u(r_v) = 7 + 14 \times 7(mod17) = 3$

$k_{u,w} = g_u(r_w) = 7 + 14 \times 1(mod17) = 4$

To get Keys of U and W ,V compute:

$k_{v,u} = g_v(r_u) = 6 + 4 \times 12(mod17) = 3$

$k_{v,w} = g_v(r_w) = 6 + 4 \times 1(mod17) = 10$

To get the Keys of V and U,W computes:

$k_{w,u} = g_w(r_u) = 15 + 9 \times 12(mod17) = 4$

$k_{w,v} = g_w(r_v) = 15 + 9 \times 7(mod17) = 10$

$\therefore$ The three keys are
$k_{u,v} = 3$
$k_{u,w} = 4$
$k_{v,w} = 10$

THEOREM

The Blom Key predistribution scheme with k=1 is unconditionally secure aganist any individual user.
Proof
Suppose that user W wants to compute the Key of U and V.
$k_{u,v} = a + b(r_u + r_v) + cr_u r_v(modp)$
Here the value of $r_u and r_v$ are public,but a,b,c are unknown.
W knowns the values,
$a_w = a + br_w(modp)$and$b_w = b + cr_w(modp)$ because these are the coefficients of the polynomial $g_w(x)$ that was sent to W by TA.
We will show that the information known by W is consistent with any possible value $k^* \in Z_P$ of the Key $k_{u,v}$.
Consider the following matrix equation,

$$\begin{pmatrix} 1 & r_u + r_v & r_u r_v \\ 1 & r_w & 0 \\ 0 & 1 & r_w \end{pmatrix} \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} k^* \\ a_w \\ b_w \end{pmatrix}$$

The determinant of the coefficient matrix is
$(r_w)^2 - (r_u + r_v)r_w + r_u r_v = r_w^2 - r_u r_w - r_v r_w + r_u r_v$
$= (r_w - r_u)r_w - r_v(r_w - r_u) = (r_w - r_u)(r_w - r_v)$
where all arithmetic done in z_p.since $r_w \neq r_u$, $r_w \neq r_v$ and p is a prime it follows that the coefficient matrix has non-zero determinant and hence the matrix equation has a unique solution for a,b and c in Z_p
$\therefore$ we have shown that any possible value k^* of $k_{u,v}$ is consistent with the information known to W.
Hence,W cannot compute $k_{u,v}$

PROTOCOL OF BLOM KEY PREDISTRIBUTION SCHEME (ARBITRARY k)

STEP 1:A prime number p is made public and for each user U, an element $r_u \in Z_P$ is made public.The elements r_u must be distinct.

STEP2: For $0 \leq i, j \leq k$.The TA choose random element $a_{ij} \in Z_P$,such that $a_{i,j} = a_{j,i} \forall i, j$
Then the TA forms the polynomial
$f(x, y) = \Sigma_{i=0}^{k} \Sigma_{j=0}^{k} a_{i,j} x^i y^j (mod p)$

STEP3: For each user U, the TA computes the polynomial
$g_u(x) = f(x, r_u)(mod p) = \Sigma_{i=o}^{k} a_{u,i} x^i$
and transmits the coefficient vector $(a_{u,o}, ..., a_{u,k})$ to U over a secure channel.

STEP4: For any two users U and V the Key $k_{u,v} = f(r_u, r_v)$,
where U computes
$k_{u,v} = g_u(r_v)$
and V computes $k_{v,u} = g_v(r_u)$

THEOREM (Lagrange Interpolation Formula)

Suppose p is prime,suppose $x_1, x_2, ..., x_{m+1}$ are distinct elements in Z_p and suppose $a_1, a_2, ..., a_{m+1}$ are elements in Z_p.Then there is a unique polynomial $A(x) \in Z_p[x]$ having degree at most m,such that $A(x_i) = a_i, 1 \leq j \leq m + 1$.
The polynomial A(x) is as follows
$A(x) = \Sigma_{i=0}^{m+1} a_j \Pi_{1 \leq h \leq m+1, h \neq j} \frac{(x - xh)}{(x_j - xh)}$

THEOREM (BIVARIATE LAGRANGE INTERPOLATION FORMULA)

Suppose p is a prime ,suppose that $x_1, x_2, ..., x_{m+1}$ are distinct elements in Z_p and suppose that $a_1(x), a_2(x), ..., a_{m+1}(x)$ are elements in $Z_p[x]$ are polynomials of degree at most m.Then there is a unique polynomial $A(x, y) \in Z_p[x, y]$ having degree at most m(in x and y),such that $A(x, y) = a_i(x), 1 \leq j \leq m + 1$..The polynomial A(x,y) is as follows
$A(x, y) = \Sigma_{j=0}^{m+1} a_j(x) \Pi_{1 \leq h \leq m+1, h \neq j} \frac{(y - yh)}{(y_j - yh)}$

EXAMPLE OF BIVARIATE LAGRANGE INTERPOLATION FORMULA

Let p=13,m=2,$y_1 = 1, y_2 = 2, y_3 = 3$
$a_1(x) = 1 + x + x^2, a_2(x) = 7 + 4x^2$ and $a_3(x) = 2 + 9x$
then
$\frac{(y-2)(y-3)}{(1-2)(1-3)} = 7y^2 + 4y + 3$

$\frac{(y-1)(y-3)}{(2-1)(2-3)} = 12y^2 + 4y + 10$

$\frac{(y-1)(y-2)}{(3-1)(3-2)} = 7y^2 + 5y + 1$

$\therefore A(x, y) = (1 + x + x^2)(7y^2 + 4y + 3) + (7 + 4x^2)(12y^2 + 4y + 10) + (2 + 9x)(7y^2 + 5y + 1)(mod 13)$
$= y^2 + 3y + 10 + 5xy^2 + 3x^2y^2 + 7x^2y + 4x^2 + 10xy + 12x$

One drawback of Blom Key Predistribution Scheme is that there is a sharp security threshold(namely,the vale of k) which be prespecified.Once more than K users decide to collaborate,the whole scheme can be broken .The BKPS is optimal with respect to its storage requirements.For any unconditionally secure Key Predistribution that is secure against coalitions of size K requires each user's storage to be atleast K+1 times the length of a key

1.2 KEY AGREEMENT BASED ON ASYMMETRIC TECHNIQUES

1.21 DIFFIE-HELLMAN KEY AGREEMENT

Diffie-Hellman Key Agreement provided the first practical solution to the Key distribution problem,allowing two parties never having met in advance or shared keying material to establish a shared secret by exchanging messages over an open channel.

PROTOCOL

The public domain parameters consist of a group (G,.) and an element $\alpha \in G$ having order n
1.U chooses a_u at random,where $0 \leq a_u \leq n-1$
Then she computes $b_u = \alpha^{a_u}$ and sends b_u to V

2.V chooses a_v at random ,where $0 \leq a_v \leq n-1$
Then he computes $b_v = \alpha^{a_v}$ and sends b_v to U.

3.U computes $K = (b_v)^{a_u}$
and V computes $K = (b_u)^{a_v}$

EXAMPLE

P=11,$\alpha = 7$,
U choose $a_u = 3$,and compute $b_u = \alpha^{a_u}(mod 11)$
$= 7^3(mod 11) = 343(mod 11) = 2$
V choose $a_v = 6$ and compute $b_v = \alpha^{a_v}(mod 11)$
$= 7^6(mod 11) = 117649(mod 11) = 4$
Then U send 2 to V and V send 4 to U
U receives 4 and compute K=$(b_v)^{a_u}(modp) = 4^3(mod 11) = 9$
V receives 2 and compute K=$(b_u)^{a_v}(modp) = 2^6(mod 11) = 9$

It is well-known that the Diffie-Hellman KAS has a disadvantage in the presence of an active adversary
For example
Suppose Diffie-Hellman KAS is work like this
U$\xrightarrow{\alpha^{a_u}}V$
U$\xleftarrow{\alpha^{a_v}}$V
Suppose W will intercept messages between U and V and add his own messages
U $\xrightarrow{\alpha^{a_u}}$ W $\xrightarrow{\alpha^{a'_u}}$ V

U $\xleftarrow{\alpha^{a'_v}}$ W $\xleftarrow{\alpha^{a_v}}$ V

At the end of the session,U has actually established the secret key $\alpha^{a_u a'_v}$ with W and V has established the secret key $\alpha^{a'_u a_v}$ with W.When U tries to encrypt a message to sent to V,W will be able to decrypt it but V will not be able to do.Similarly V tries to encrypt a message to sent to U,W will able to decrypt but U will not able.So it is essential for U and V to make sure that they are exchanging the messages with each other and not with W.To avoid such suitations design a Key agreement scheme that authenticates the participants identities at the same time as the Key is being established.A KAS of this type will be called an Authenticated Key Agreement Scheme.

1.22 ELGAMAL KEY AGREEMENT IN ONE-PASS

ElGamal proposed a public key cryptosystem in 1985.Elgamal key agreement is a Diffie-Hellman variant providing a one-pass protocol with unilateral key authentication,provided the public key of the recipient is known to the originator a priori.

PROTOCOL

To generate a key pair,first choose a prime p and two random numbers g and x such that $g < pandx < p$ .Then compute
$y \equiv g^x(modp)$
The public key is (y,g,p) and the private key is x.
To encrypt the message m,$0 \leq m \leq p-1$,first we choose a random number k such that gcd (k,p-1)=1.The encrypted message is then the following pair (r,s):
$r \equiv g^x(modp)$
$s \equiv (y^k(modp))(m(modp-1))$
Note that the size of the ciphertext is double the size of the message.To decrypt the message,divide s by r^x.
$r^x \equiv (g^k)^x(modp)$
$s/r^x \equiv y^k m/(g^k)^x \equiv (g^x)^k m/(g^k)^x \equiv m(modp-1)$

EXAMPLE

Choose :p=11,g=4,x=8
Then compute
$y \equiv g^x(modp) \equiv 4^8(mod11) \equiv 9$
The public key is 9.The private key x= 8.To encrypt the message m=5,first choose a random number k=7,such that gcd(7,10)=1 and compute:
$r \equiv g^k(modp) \equiv 4^7(mod11) \equiv 5$
$s \equiv (y^k(modp))(m(modp-1)) \equiv (9^7(mod11))(5(mod10)) \equiv 4 \times 5 \equiv 20$
To decrypt the message m,first compute:
$r^x(modp) \equiv 5^8(mod11) \equiv 4$
then
$m = s/r^x(modp) \equiv 20/4 \equiv 5$

1.23 MTI KEY AGREEMENT SCHEMES

Matsumoto,Takashima and Imai have constructed several interesting key agreement schemes by modifying the Diffie-Hellman KAS .Which we call MTI Schemes.They also termed as two-flow or pass key agreement schemes,because they are only two separate transmissions of information performed in each session of the scheme.

PROTOCOL:MTI/A0

The public domain parameters consist of a group (G,.) and an element $\alpha \in G$ having order n.Each user T has a secret exponent a_T where $0 \leq a_T \leq n-1$ and corresponding public vale $b_T = \alpha^{a_T}$ The vale b_T is included in T's certificate and is signed by the TA.

1.U choose r_u at random ,$0 \leq r_u \leq n-1$ and computes $s_u = \alpha^{r_u}$.Then U sends Cert(U) and s_u to V

2.V chooses r_v at random,$0 \leq r_v \leq n-1$ and compute $s_v = \alpha^{r_v}$ Then V sends Cert(V) and s_v to U.
Finally V computes the session key
$K = s_u^{a_v} b_u^{r_v}$,
where he obtains the vale b_u from Cert(U).

3.U compute the session key
$K = s_v^{a_u} b_v^{r_u}$
wher she obtains the value b_v from Cert(V).

At the end of the session,U and V have both computed the same session key
$K = \alpha^{r_u a_v + r_v a_u}$

EXAMPLE

Suppose p=27803,n=p-1=270802 and $\alpha = 5$.The public domain parameters for the scheme consist of the group $(Z_p^*, .)$ and α
Assume U chooses a secret exponent $a_u = 21131$
then she will compute
$b_u = 5^{21131} (mod 27803) = 21420$

which is placed on her certificate.
Then V chooses a secret exponent
$a_v = 17555$ then he will compute

$b_v = 5^{17555}(mod 27803) = 17100$
which is placed on his certificate.

Now suppose that U chooses $r_u = 169$.
then she will send the value

$s_u = 5^{169}(mod 27803) = 6268$ to V.
Suppose that V chooses $r_v = 23456$
then he will send the value,

$s_v = 5^{23456}(mod 27803) = 26759$

Now U can compute the key

$K_{U,V} = s_v^{a_u} b_v^{r_u}(mod p) = 26759^{21131} \times 17100^{169} = 21600$

and V can compute the key

$K_{V,U} = s_u^{a_v} b_u^{r_v}(mod p) = 6258^{17555} \times 21420^{23456}(mod 27803) = 21600$

ATTACKS ON MTI/A0

1.Known session key attacks on MTI/A0

The adversary W is an active participant in two sessions,W pretends to be V in a session S with U and W pretends to be U in a parallel session S' with V.The actions taken by W are illustrated as in figure 1.

The flows in the two sessions are lebeled in the order in which they occur (1) and (2) represent the initial flows in the sessions S' and S,respectively.Then the information in flow (1) is copied to flow (3),and the information in flow(2) is copied to flow(4) by W.Since the two sessions are being executed in parallel ,we have a parallel session attack.W requests the key K for session S',which he is allowed to do in a known session key attack ofcouse K is also the key

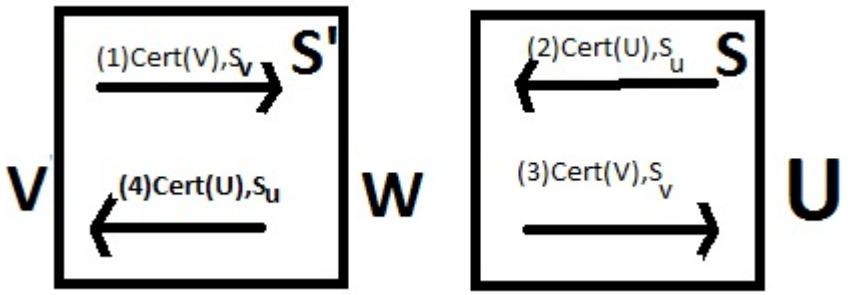
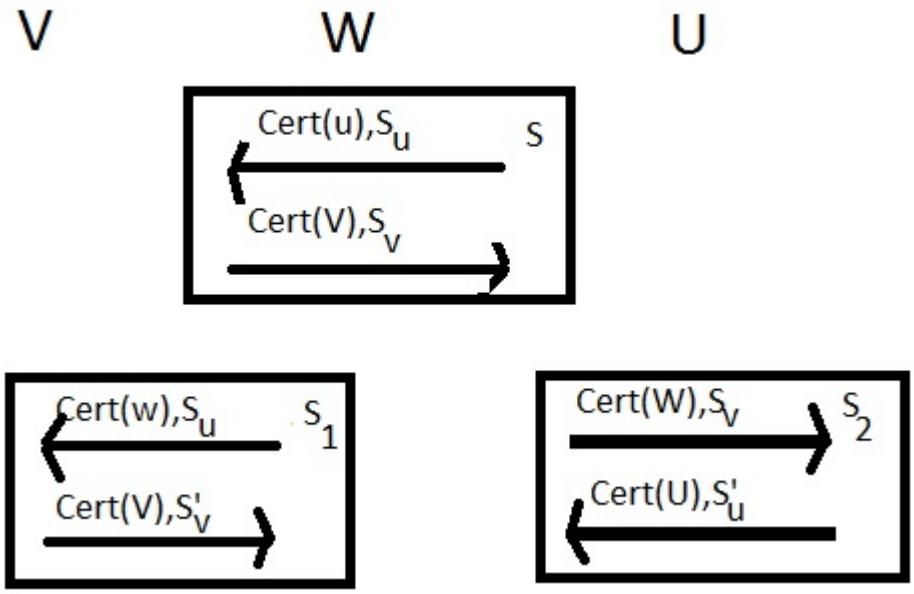


Figure 1:

for session S, so W achieves his goal of computing the key for a session in which he is an active adversary.The parallel session attack can be carried out because the key is a symmetric function of the input provided by the two parties.
$K((r_u, a_u), (r_v, a_v)) = K((r_v, a_v), (r_u, a_u))$
To eliminate the attack,we should destroy this symmetric property.This could be done by using a hash function h as a key derivation function.
Suppose that the actual session key K was defined to be$K = h(\alpha^{r_u a_v} \parallel \alpha^{r_v a_u})$
U(the initiator of the session) would compute
$K = h(b_v^{r_u} \| s_v^{a_u})$
While V(the responder of the session)would compute
$K = h(s_u^{a_v} \| b_u^{r_v})$
with this modified method of constructing a session key, the attack no longer works, because two sessions S and S' how have different keys.
The key for session S is
$K_S = h(\alpha^{r_u a_v} \| \alpha^{r_v a_u})$
For S'
$K_{S'} = h(\alpha^{r_v a_u} \| \alpha^{r_u a_v})$.

BURMESTER TRIANGLE ATTACK



First W observes a session S between U and V.Then W participates in two additional sessions S_1 and S_2 with U and V respectively.In these two sessions,W transmits values S_u and S_v that are copied from S.(W does not know the exponents r_u andr_v corresponding to S_u and S_v) Then after the sessions S_1 and S_2 have concluded,W requests the key for these two session,which is permitted in a known session key attack.
The session keys K,$K_1$and K_2 for the sessions S, S_1 and S_2 are given by
$K = \alpha^{r_u a_v + r_v a_u}$
$K_1 = \alpha^{r_u a_v + r_v^{'} a_w}$
$K_2 = \alpha^{r_u^{'} a_w + r_v a_u}$
Given $K_1$and K_2 ,W is able to compute K
$K = \dfrac{K_1 K_2}{(S_v^{'} S_u^{'})^{a_w}}$

The triangle the use the key derivation function.

1.24 THE STATION-TO-STATION KEY AGREEMENT SCHEME(STS)

This is an authenticated key agreement scheme which is a modification of the Diffie-Hellman KAS.The scheme makes use of certificates which as usual, are signed by a TA.Each user U will have a signature scheme with a verification algorithm Ver_U and a signing algorithm Sig_U.The TA also has a signature scheme with a public verification algorithm Ver_{TA}.Each user U has a certificate
$Cert(U) = (ID(U), Ver(U), Sig_{TA}(ID(U), Ver_U)$
Where ID(U) is certain identification information for U.

PROTOCOL
The public domain parameters consist of a group (G,.) and an element $\alpha \in G$ having order n.

1.U choose a random number $a_u, 0 \leq a_u \leq n-1$.
Then she computes$b_u = \alpha^{a_u}$
and she sends Cert(U) and b_u to V.

2.V chooses a random number $a_v, 0 \leq a_v \leq n-1$.
Then he computes $b_v = \alpha^{a_v}$
$K = (b_u)^{a_v}$ and
$y_v = Sig_v(ID(U) \| b_v \| b_u)$
Then V sends Cert(V),b_v and y_v to U.

3.U verifies y_v using Ver_V.iF the signature y_v is not valid,then she "rejects" and quits otherwise,she "accepts"
she computes $K = (b_v)^{a_u}$ and $y_u = Sig_U(ID(U) \| b_u \| b_v)$
and she sends y_u to V

4.V verifies y_u using Ver_U if the signature y_u is not valid,then he "rejects" and quits otherwise,he "accepts".

CHAPTER 2

KEY TRANSPORT

2.1 KEY TRANSPORT BASED ON SYMMETRIC ENCRYPTION

2.11 KERBEROS

Kerberos comproses a popular series of schemes for session key distribution that were developed at MIT in the late 1980's and early 1990's.The basic Kerberos protocol involves A(the client),B(the server and verifier) and a trusted sever TA(the Kerberos authentication sever).At the out set A and B share no secret,while T shares a secret with each.(eg:a user password etc.).The primary objective is for B to verify A's identity.The establishment of a shared key is a side effect.Options include a finial message providing mutual entity authentication and establishment of a additional secret shared by A and B.

PROTOCOL:Simplified Kerberos v5

1. Alice chooses a random number r_A.Alice sends ID(Alice),ID(Bob) and r_A to TA.

2. The TA chooses a random session key K and a validity period(or life time),L.
Then it compute a ticket to Bob.
$t_{Bob} = e_{K_{Bob}}(K \| ID(Alice) \| L)$
and
$y_1 = e_{K_{Alice}}(r_A \| ID(Bob) \| K \| L)$
The TA sends t_{Bob} and y_1 to Alice.

3. Alice decrypts y_1 using her key K_{Alice} obtaining K.Then Alice determine the current time and she computes
$y_2 = e_K(ID(Alice) \| time)$.
Finally Alice sends t_{Bob} and y_2 to Bob.

4. Bob decrypts t_{Bob} using his key K_{Bob} obtaining K.He also decrypts y_2 using the key K,obtaining time.Then Bob computes

$y_3 = e_K(time + 1)$

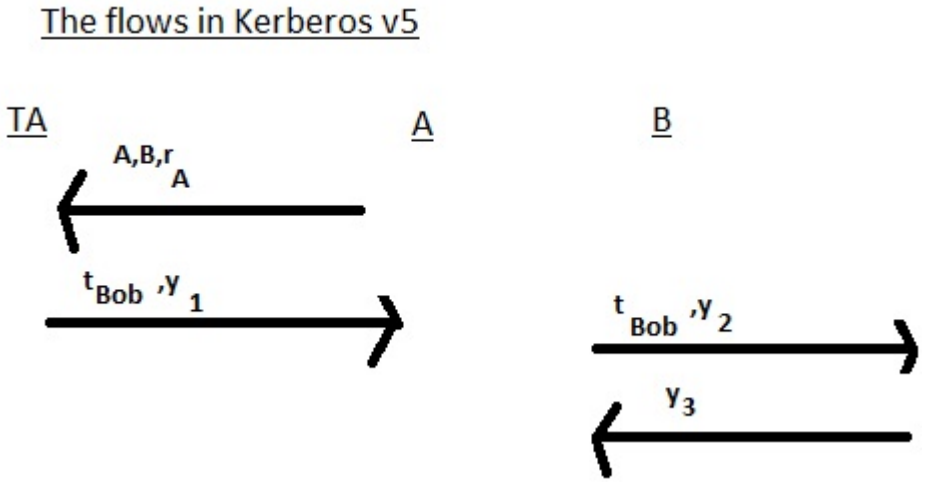
Finally Bob sends y_3 to Alice.

The purpose of the lifetime L is to prevent an active adversary from storing "old" messages for retransmission at a later time.
One of the drawbacks of Kerberos is that all the users int the network should have synchronized clock,since the current time is used to determine if a given session key K is valid.In practice,it is very difficult to provide perfect synchronization,so some amount of variation in time must be allowed.

There are certain validity checks are also required in Kerberos.
They are as follows:
1. When Alice decrypts y_1 ,she checks to see that the plain text $d_{K_{Alice}}(y_1)$ has the form
$d_{K_{Alice}} = r_A \| ID(Bob) \| K \| L.$
for some K and L.
If this condition does not hold,then Alice "rejects" and aborts the current session.

2. When Bob decrypts y_2 and t_{Bob} ,he checks to see that the plain text $d_K(y_2)$ has the form
$d_K(y_2) = ID(Alice) \| time$ and the plain text $d_{K_{Bob}}(t_{Bob})$ has the form
$d_{K_{Bob}}(t_{Bob}) = K \| ID(Alice) \| L$
Where ID(Alice) is the same in both plain text and time L.If these condition hold,then Bob "accepts",otherwise Bob "rejects"

3. When Alice decrypts y_3,she checks that $d_K(y_3) = time+1$. If this condition holds,then Alice "accepts",otherwise Alice "rejects".



Where,
A=ID(Alice)
B=ID(Bob)
$t_{Bob} = e_{K_{Bob}}(K \| A \| L)$
$y_1 = e_{K_{Alice}}(r_A \| B \| K \| L)$
$y_2 = e_K(A \| time)$
and
$y_3 = e_K(time + 1)$

2.12 THE NEEDHAM-SCHROEDER SCHEME

It was proposed in 1978.It is an example of a protocol independent of time stamps,providing both entity authentication assurances and key establishment with key confirmation.

PROTOCOL:

1. Alice choose a random number r_A.Alice sends ID(Alice),ID(Bob) and r_A to the TA.

2. The TA chooses a random session key K.
Then it computes:
$t_{Bob} = e_{K_{Bob}}(K \| ID(Alice)$
(Which is called a ticket to Bob) and
$y_1 = e_{K_{Alice}}(r_A \| ID(Bob) \| K \| t_{Bob})$
and it sends y_1 to Alice

3. Alice decrypts y_1 using her key K_{Alice} obtaining K and t_{Bob}.Then Alice sends t_{Bob} to Bob.

4. Bob decrypts t_{Bob} using his key K_{Bob} obtaining K,Then Bob chooses a random number r_B and computes
$y_2 = e_K(r_B)$
Bob sends y_2 to Alice.

5.Alice decrypts y_2 using the key K,obtaining r_B.Then Alice computes
$y_3 = e_K(r_B - 1)$ and she sends y_3 to Bob.

There are also some validity checks to verifying in the Needham-Schroeder scheme.
1. When Alice decrypts y_1,she checks to see that the plain text $d_{K_{Alice}}(y_1)$ has the form
$d_{K_{Alice}}(y_1) = r_A \| ID(Bob) \| K \| t_{Bob}$
for some K and t_{Bob}.If this condition does not hold,then Alice "rejects" and aborts the current session,otherwise she "accepts".

2. When Bob decrypts y_3 he checks to see that the plain text
$d_K(y_3) = r_B - 1$
If these condition hold,then Bob "accepts",otherwise Bob "rejects".

2.2 KEY TRANSPORT BASED ON PUBLIC KEY ENCRYPTION

Key transport based on public key encryption involves one party choosing a symmetric key and transferring it to a second,using that party's encryption public key.

2.21 NEEDHAM-SCHROEDER PUBLIC KEY PROTOCOL

The Needham-schroeder public key protocol provides mutual entity authentication and mutual key transport.The transported keys may serve both as nonces for entity authentication and secret keys for further use.Combination of the resulting shared keys allows computation of a joint key to which both parties contribute.

PROTOCOL:

NOTATIONS:
$P_X(Y)$ denotes public key encryption of data Y using party X's public key.
$P_X(Y_1, Y_2)$ denotes the encryption of the concatenation of Y_1 and Y_2 .K_1 and K_2 are secret symmetric session keys chosen by A and B.

a) A sends B the message $P_B(K_1, A)$

b) B recovers K_1 upon receiving message and returns to A message $P_A(K_1, K_2)$

c) Upon decrypting message $P_A(K_1, K_2)$,A checks the key K_1 recovered agree with that sent in message $P_B(K_1, A)$ (provided K_1 has never been previously used,this gives A both entity authentication of B and assurance that B knows this key).A sends $P_B(K_2)$ to B.

d) Upon decrypting the message $P_B(K_2)$,B checks the key K_2 recovered agrees with that sent in message $P_A(K_1, K_2)$.The session key may be computed as $f(K_1, K_2)$ using an appropriate publicly known non-reversible function f.

CHAPTER 3

KEY MANAGEMENT LIFE CYCLE

Key management is simplest when all cryptographic keys are fixed for all time.Cryptoperiods necessitate the update of keys.The set of stages through which a key progress during its existence,referred to as the life cycle of keys. The sequence of states which keying material progresses through over its lifetime is called the key management life cycle.

Life cycle stages

1.User registration
2.User initialization
3.Key generation
4.Key installation
5.Key registration
6.Normal use
7.Key backup
8.Key update
9.Archival
10.Key de-registration and destruction
11.Key recovery
12.Key revocation

1.User registration:

An entity becomes an authorized member of a security domain.This involves acquisition,or creation and exchange,of initial keying material such as shared password or PINs by a secure one-time technique

2.User initialization:

An entity initializes its cryptographic application(eg;installs and initializes software or hardwares) involving use or installation of initial keying material obtained during user registration.

3.Key generation

Generation of cryptographic keys should include measures to ensure appropriate properties for the intended application or algorithm and randomness in the sence of being predictable with negligible probability.An entity may generate its own keys or acquire keys from a trusted system component.

4.Key installation

Keying material is installed for operational use within an entity's software or hardware,by a variety of techniques including one or more of the following
Manual entry of a password or PIN
Transfer of a disk
Read-only-memory device
Chipcard or other hardware token or device.
The initial keying material may serve to establish a secure on-line session through which working keys are established.During subsequent updates new keying material is installed to replace that in use,ideally through a secure on-line update technique.

5.Key registration:

In association with key installation,keying material may be officially recorded as associated with a unique name which distinguish an entity.For public keys,public-key certificates may be created by a certification authority and made available to others through a public directory or other means.

6.Normal use

The objective of the life cycle is to facilitate operational availability of keying material for standard cryptographic proposes.Under normal circumstances,this state continues until crypto period expiry.It may also be subdivided -eg for encryption public key pairs, a point may exist at which the public key is no longer deemed valid for encryption,but the private key remains in (normal) use for decryption.

7.Key backup

Backup refers to short-term storage during operational use.Backup of keying material in independent,secure storage media provides a data source for key recovery.

8.Key update

Prior to cryptoperiod expiry,operational keying material is replaced by new material.This may involve some combination of key generation,key derivation,execution of two-party key establishment protocols or communication with a trusted 3^{rd} party.For public keys,update and registration of new keys typically involves secure communications protocol with certification authorities.

9.Archival

Archival refers to off-line long-term storage of post-operational keys.Keying material no longer in normal use may be archived to provide a source for key retrieval under special circumstances (eg:settling disputes involving repudiation).

10.Key-deregistration and destruction

Once there are no further requirements for the value of a key or maintaining its association with an entity,the key is de-registered (removed from all official record of existing keys),and all copies of the key are destroyed.In the case of secret keys,all traces are securely erased.

11.Key recovery

If keying material is lost in a manner free of compromise (eg:due to forgotten passwords),it may be possible to restore the material from a secure backup copy.

12.Key revocation

It may be necessary to remove keys from operational use prior to their originally scheduled expiry,for reasons including key compromise.For public key distributed by certificates,this involves revoking certificates.

Of the above stages,all are regularly scheduled,except key recovery and key revocation which arise under special situations.

CONCLUSION

Cryptography helps us to make a secure communication in public networks.The secret key plays an essential role in the cryptosystems such that revealing the secret key causes the cryptographic system to be compromised.Therefor how the exchange of the secret key takes place is very important in cryptographic applications.One of the considerable methods for secret key exchange is the key agreement protocols.These protocols enable two or more users of any public network to share a secret common key together.

The main focus of this project is on Key Establishment Protocols as cryptographic primitives,because they are the most important and the hardest to construct.The most important primitive of public key cryptosystem is the key agreement protocols,which enables a network of users to exchange a common shared key for their cryptographic uses.Thus the research on cryptography changed its direction from private key cryptosystems to public key cryptosystems.

With the rapid usage of data communication from e-mail to cellular communications, from secure web access to digital cash,security is becoming a more crucial issue.Cryptography can use to secure the data.The essential necessities for security incorporate confidentiality,validation,intergrity, and non-renouncement.To give such security administrations,most framework uses two noteworthy classes of cryptographic algorithms to be specific symmetric key and public key algorithms.Symmetric algorithms are speedier than asymmetric yet have a few disadvantages like absence of scalability,troublesome key administration and give just privacy.The asymmetric algorithms permit public key foundation and key trade frameworks,however at the expense of speed.

Also doing this project we seen different key transport protocols such as Kerberos,Needham-schoeder etc.Finally we have seen different stages of a key.Many more concepts from cryptography remain unexplored for key establishment,and we hope that our work will stimulate more research in this area.

REFERENCE

[1]Alfred J Menezes,Paul C Van Orschot,Scott A Vanstone:Handbook of applied Cryptography

[2] William Stalling:Cryptography and network security

[3] Douglas R Stinson: Cryptography Theory and Practice third edition

[4] Eddie M.Ng:Security Models and Proofs for Key Establishment Protocols.

[5] Man Young Rhee:Internet Security Cryptographic Principles,Algorithms and Protocols.

[6] Bruce Schneier:Applied Cryptography