**Unit-II: Public Key Cryptography**

**Session -1: Key management Date: 23.07.2013 Period: 01**

* **Introduction to key management-presentation**

**(http://www1.cse.wustl.edu/~ychen/505A/Slides/ch10.ppt)**

* **Distribution of Public keys**
* Public announcement of public keys
* Publicly available directory
* Public key authority
* Public key certificates
* **Show and tell**

**Public announcement of public keys**: The below diagram show the meaning of public announcement – all user public keys are distributed publicly.

** **

* **Show and tell**

**Publicly available directory:** In this method user’s public keys registered like telephone directory.

****

**Conclusion: Ask any one learner summarizes the above contents.**

**Session – 2 : Key management Date: 23.07.2013 Period: 05**

* **Show and tell**

**Public key authority:** From the diagram, learners can understand the key authority

****

****

Public key certificate, Distribution of secret keys and hybrid scheme: **Presentation**

**(http://www1.cse.wustl.edu/~ychen/505A/Slides/ch10.ppt)**

Conclusion: Group Quiz

Activity Description: We can divide the learners into two teams and instruct each team to prepare 5 questions on the Feedback and its types. After 5 minutes of preparation, each team will ask the other team the questions prepared.

**Session – 3: Diffie- Hellman key exchange algorithm Date: 24.07.2013 Period: 02**

* **Video clipping :** [**http://www.youtube.com/watch?v=40i9ujVJ040**](http://www.youtube.com/watch?v=40i9ujVJ040)

**:** [**http://www.youtube.com/watch?v=3QnD2c4Xovk**](http://www.youtube.com/watch?v=3QnD2c4Xovk)

**Presentation : (http://www1.cse.wustl.edu/~ychen/505A/Slides/ch10.ppt)**

* **Board Activity: Choose any learner and insist to do problem in board**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | |  |  |  |  |  |  |  | |  |  |

* users Alice & Bob who wish to swap keys:
* agree on prime q=353 and a=3
* select random secret keys:
  + A chooses xA=97, B chooses xB=233
* compute respective public keys:
  + yA=397  mod 353 = 40 (Alice)
  + yB=3233 mod 353 = 248 (Bob)
* compute shared session key as:
  + KAB= yBxA mod 353 = 24897 = 160 (Alice)
  + KAB= yAxB mod 353 = 40233 = 160 (Bob)

Conclusion: Group Quiz

* Activity Description: We can divide the learners into two teams and instruct each team to prepare 5 questions on the Feedback and its types. After 5 minutes of preparation, each team will ask the other team the questions prepared.

**Session -4: Elliptic curve cryptography Date: 25.07.2013 Period: 04**

**Presentation (content): http://www1.cse.wustl.edu/~ychen/505A/Slides/ch10.ppt**

**Board Explanation**

* can do key exchange analogous to D-H
* users select a suitable curve Ep(a,b)
* select base point G=(x1,y1)

with large order n s.t. nG=O

* A & B select private keys nA<n, nB<n
* compute public keys: PA=nAG, PB=nBG
* compute shared key: K=nAPB,K=nBPA

same since K=nAnBG

* several alternatives, will consider simplest
* must first encode any message M as a point on the elliptic curve Pm
* select suitable curve & point G as in D-H
* each user chooses private key nA<n
* and computes public key PA=nAG
* to encrypt Pm : Cm={kG, Pm+kPb}, k random
* decrypt Cm compute:

Pm+*k*Pb–nB(*kG*) = Pm+*k*(nB*G*)–nB(*kG*) = Pm

**Conclusion: Group Quiz**

* Activity Description: We can divide the learners into two teams and instruct each team to prepare 5 questions on the Feedback and its types. After 5 minutes of preparation, each team will ask the other team the questions prepared.

**Session -5: Introduction to number theory Date: 27.07.2013 Period: 07**

**Recap: Question and answer**

1. What is prime number?

An integer P > 1 is a prime number if and only if its only divisor are +1, -1 and +P,-P.

1. Give examples of prime number .

3,5,7,11,13,17,19….

**Content : Fermat’s Theorem and Chinese remainder theorem**

Activity: Presentation slides {http://mercury.webster.edu/aleshunas/COSC%205130/ch08.ppt}

**Conclusion :** Summarization by learners

Ask any one learner summarizes the above contents.

**Session -6 Confidentiality using symmetric encryption Date: 29.07.2013 Period : 03**

**Recap: Presentation {http://www1.cse.wustl.edu/~ychen/505A/Slides/ch10.ppt}**

**Content: Key distribution scenario &Hierarchical key control**

Presentation slides: http://www.eecis.udel.edu/~mills/teaching/eleg867b/crypto\_slides/ch07.ppt

**Conclusion: Questions and answers**

1. **List ways in which secret keys can be distributed to two communicating parties.**

* + A can select a key and physically deliver it to B.
  + A third party can select the key and physically deliver it o A and B
  + If A and B have previously and recently used a key, one party can transmit the

new key to the other, encrypted using the old key

* + If A and B each has an encrypted connection to a third party C, C can deliver a

key on the encrypted links to A and B

2. **What is nonce?**

Consider A issues a request to the KDC for a session key to protect a logical connection to B. The message includes the identity of A and B and a unique identifier, N1, for this transaction, which we refer to as nonce. The nonce may be a timestamp, a counter, or a random number

3. **What is key distribution center?**

* A key distribution center is responsible for distributing keys to pairs of users such as hosts, processes, applications. Each user must share a unique key with the key distribution center for purposes of key distribution.

4. **Specify the application of public key cryptography.**

Encryption/Decryption.

Digital signature.

Key exchange.

**Session -7 Confidentiality using symmetric encryption Date: 30.07.2013 Period: 01**

**Recap: Group quiz**

* Activity Description: We can divide the learners into two teams and instruct each team to prepare 5 questions on the Feedback and its types. After 5 minutes of preparation, each team will ask the other team the questions prepared.

**Unspoken activity:**

Show the Picture and learners can understand the content of topic

http://www.eecis.udel.edu/~mills/teaching/eleg867b/crypto\_slides/ch07.ppt


Ch07. KDC.pdf                                                  00156198  Mnementh                      BEAE7A2F:

**Conclusion:**

**Recall by words**

Digital signature,

Key exchange,

**key distribution center,**

**NONCE (Number ONCE),**

**Session -8 Random number generation Date: 30.07.2013 Period: 04**

**Recap:** Recall by keywords

Secrete key, nonce, Identity of user – in this topic random number used.

**Content : Pseudorandom number generator & Blum Blum shub generator**

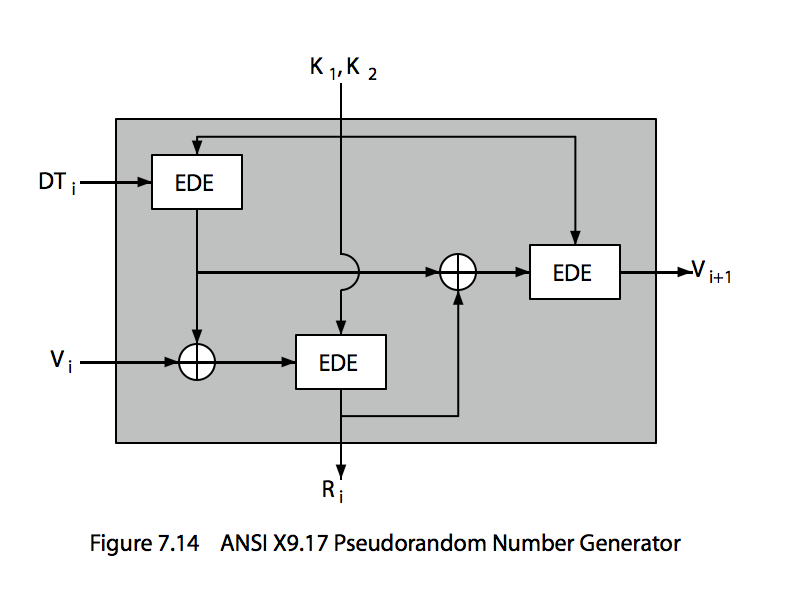
Presentation slides: http://www.eecis.udel.edu/~mills/teaching/eleg867b/crypto\_slides/ch07.ppt

**Conclusion: Questions and answers**

1. What is iterative expression of Linear Congruential Generator?

*Xn*+1 = (*a X*n + *c*) mod *m*

1. Draw the ANSI random number generator?



1. What is meant by Blum Blum Shub generator?

use least significant bit from iterative equation:

* 1. x*i* = x*i-1*2 mod n
  2. where n=p.q, and primes p, q=3 mod 4

1. What are applications of Random numbers in cryptography?

many uses of **random numbers** in cryptography

* 1. nonces in authentication protocols to prevent replay
  2. session keys
  3. public key generation
  4. keystream for a one-time pad

**Session -9 Public key cryptography Date: 31.07.2013 Period: 01**

**Recap: Presentation {http://faculty.mu.edu.sa/public/uploads/1366440153.2306ch09.ppt}**

**Content: Public key cryptosystem & Public key secrecy and Confidentiality**

**Presentation slides: http://faculty.mu.edu.sa/public/uploads/1366440153.2306ch09.ppt**

**Conclusion :** Questions and answers

1. **Differentiate public key encryption and conventional encryption.**

**Conventional Encryption**

1. The same algorithm with the same

2. The sender and receiver must share

3. The key must be secret

**Public key Encryption**

1.One algorithm is used for encryption Key is used for encryption and decryption and decryption with a pair of keys, one for encryption and another for decryption

2.The sender and receiver The algorithm and the key must each have one of the Matched pair of keys

3.One of two keys must be kept Secret

1. **What are roles of public and private key?**

The two keys used for public-key encryption are referred to as the public key and the private key. Invariably, the private key is kept secret and the public key is known publicly. Usually the public key is used for encryption purpose and the private key is used in the decryption side.

1. **What is a trapdoor one way function?**

A trapdoor one way function is a family of invertible functions fk, such that Y= fk( X) easy, if k and X are known X=fk -1(Y) easy, if k and y are known X= fk -1(Y) infeasible, if Y is known but k is not known.

1. **What is a public key certificate?**

The public key certificate is that used by participants to exchange keys without contacting a public key authority, in a way that is as reliable as if the keys were obtained directly from the public-key authority. Each certificate contains a public key and other information, is created by a certificate authority, and is given to a participant with the matching private key.

1. **List four general characteristics of schema for the distribution of the public key?**

The four general characteristics for the distribution of the public key are

1. Public announcement

2. Publicly available directory

3. Public-key authority

4. Public-key certificate

**Session -10 RSA algorithm Date: 03.08.2013 Period: 07**

RSA public key algorithm - Video Lecture ( <http://www.youtube.com/watch?v=tXXnHXslVhw> , <http://www.youtube.com/watch?v=ejppVhOSUmA> )

Board activity: **RSA Example - Key Setup**

1. Select primes: *p*=17 & *q*=11
2. Compute *n* = *pq* =17 x 11=187
3. Compute ø(*n*)=(*p–*1)(*q-*1)=16 x 10=160
4. Select e:gcd(e,160)=1; choose *e*=7
5. Determine d: *de=*1 mod 160 and *d* < 160 Value is d=23 since 23x7=161= 10x160+1
6. Publish public key PU={7,187}
7. Keep secret private key PR={23,187}

* sample RSA encryption/decryption is:
* given message M = 88 (nb. 88<187)
* encryption:

C = 887 mod 187 = 11

* decryption:

M = 1123 mod 187 = 88

Recap: Group quiz

* Activity Description: We can divide the learners into two teams and instruct each team to prepare 5 questions on the Feedback and its types. After 5 minutes of preparation, each team will ask the other team the questions prepared.