Suggested Teaching Guideline for
Public Key Infrastructure PG-DITISS September 2022

Duration: 30 classrooms hrs + 20 lab hrs (Total: 50 Hrs)

Objective: To introduce the student to PKI

concepts. Evaluation method: Theory exam –

40% weightage

Lab exam – 40% weightage
Internal Assessment – 20% weightage

List of Books / Other training material

Courseware: Cryptography & Network Security: Principles and Practices

Reference:

- Cryptography & Network Security – Atul Kahate
- Understanding Digital Signatures: Establishing Trust Over the Internet and OtherNetworks – Gail Grant
- Windows Server 2008 PKI and Certificate Security [With CDROM] by Brian Kumar

Note: lab sessions are of duration 4 hrs.

Session 1:

- Information Security
- Security Attacks & Threats

Session 2:

- Basic Encryption Concepts
- File Encryption
- Encryption Folders (Graphical/ using cipher)

Session 3:

- Cryptographic Fundamentals
- Cryptographic Ciphers (Symmetric and Asymmetric)
- Protocols (History, Usage, Key generation, Ciphering message)

Session 4:

Symmetric Key Encryption

- DES
- AES, RC5

Asymmetric Key Encryption

- RSA
- ECC

Session 5:

- Diffie-Hellman Key Exchange
- Attacks against encryption
- Cryptographic issues

Lab Assignments:

Using Cryptool

- Symmetric and Asymmetric key encryption and decryption
- Symmetric key encryption such as Caesar, Vernam, DES, RC4, AES, Substitution, XOR, Triple DES, etc.
- Asymmetric key encryption using RSA, ECC

Session 6:

Secure Hashing Methods

- SHA Secure Hash algorithm
- HMAC

Session 7:

PKI Fundamentals

- Digital Signature
- Digital Certificate

Session 8:

- CA
- Trust Model
- Certificate Issuance Process
- Certificate Revocation (CRL, OCSP)
- Types and Classes of Certificate

Session 9:

- Introduction to Aadhaar and e-Sign
- Time stamping Services

Lab:

Using XCA to create a Digital signature

- Digitally Sign a Word document using the created certificate
- Digitally Sign a PDF document using the created certificate

Session 10:

Public Key Cryptography Standards

- PKCS
- FIPS 140-2

Lab:

Using XCA to create a Digital certificate

- Create a digital certificate using XCA tool
  - Create CA using XCA first and then CA will issue certificate to website using XCA.
    a. Use certificate for host website (https://www.ditiss.local)
    b. Import it client browser to remove the self-signed certificate warning.

Session 11:

- Strong Authentication
- Single Factor and Multi-factor authentication
- Single Sign-on Solutions
- Open-ID and OAUTH
- Graphical Passwords

Session 12:

- Authentication Protocols
- FIDO Authentication
- Zero Trust Architecture

Session 13:

Securing Websites and Emails

- SSL
- TLS
- PGP and S/MIME

Lab:

Using OpenSSL to create

- Creating self-signed Digital Certificates using OpenSSL.
- Creating digital certificate of Hierarchical Trust Model for Intranet
  - Setup a PKI infrastructure using openssl as following:

>> Root CA (on a Debian OS - rtca.pgditiss.local)
>> Sub CA (on a Debian OS - sbca.pgditiss.local)

Setup a HTTPS website (https://www.pgditiss.local) on Apache and access the same from the windows base machine.

Note:
>> The Certificate for www.pgditiss.local to be issued by sbca.pgditiss.local
>> Configure DNS / Name Resolution as required.

Session 14 & 15:

- IT Act
- LDAP or Active Directory
- Introduction to Blockchain

Lab

- Digitally Sign and Encrypt Email using the created certificate through Email Clients like Thunderbird or Windows Mail / Outlook.