BITS, Pilani-Dubai ,
International Academic city
IV Year Second Semester 2009-10
Degree:B.E.(Hons) Branch:C.S.E

COURSE NO. : CS UC441

Selected topics from computer science

Date:29th Dec 2009 **Total marks=40 (closed book) Weightage=40%**

Compre exam **Answer all the questions Time- 3 hrs**

Answer all the questions in Part A and Part B

Part A (5 * 10 =50 Marks)

Q1. a) What is meant by dynamic html and how it can be accomplished ? (3M)

. b) I want to develop a web application in such a way that when I go to the home page it should display a web form prompting the users to enter the name and password. Once client submits the name and password the employee ID would have returned from the web server and gets displayed on the browser.. Even if the server is busy, on submission of the form no hour glass waiting cursor should be seen by the client. Outline a mechanism to achieve the same.(7M)

Q2. Microsoft wants to publish its web service by name weatherforecast in the UDDI. Its business has been categorized in the following ways given below.(10 M)

It has a DUNs number of = 99999 and under NAICS it is categorized as name = Soft ware products and value =35550

Now briefly outline the steps involved in publishing its web service in UDDI registry. The WSDl document of the web service is located in http://www.microsoft.com/weatherforecast.wsdl . The URL for the web service is http://www.microsoft.com/weatherforecast . Make any necessary valid assumptions

Q3 . Consider Alice and Bob involved in secured XML communication using hybrid key cryptography. Alice wants to transfer the given XML document with the selective encryption of **Number element.** Outline the steps involved in doing the same including key exchange mechanisms. (10M)

```
<?xml version='1.0'?>
    <PaymentInfo xmlns='http://example.org/paymentv2'>
     <Name>John Smith<Name/>
     <CreditCard Limit='5,000' Currency='USD'>
      <Number>4019 2445 0277 5567</Number>
      <Issuer>Bank of the Internet</Issuer>
      <Expiration>04/02</Expiration>
     </CreditCard>
    </PaymentInfo
```

Q4. a) Outline how SSL communication takes place between a web browser client and a web server.(6M)

b)Outline with the help of a diagram the AH type of security.(4M)

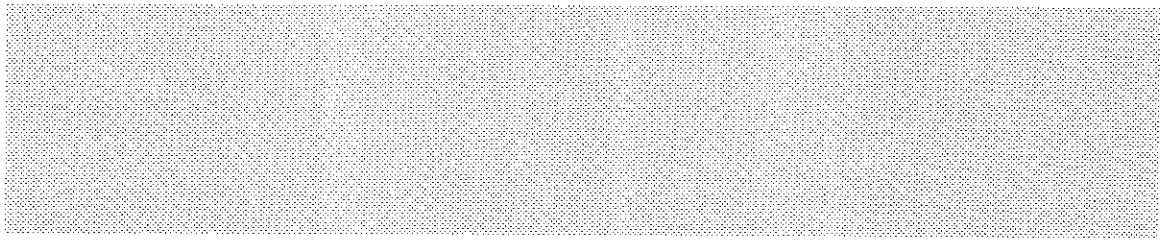
Q5. Outline how using DOM parser and sax parser the attributes of the following xml documents are got ?(5+5M)

```
<author>
  <name>
    <first> Art </first>
    <last> Gittleman </last>
  </name>
       <book type="text">
        <title full="false">Computing with Java</title>
        <edition> second </edition>
        <copyright> 1998, 2001 </copyright>
        <isbn> 1-57676-023-5 </isbn>
     </book>
</author>
```

Part- B (5 * 4 =20Marks)

Q1.How using web service, interoperability between a client and service running on heterogeneous platforms can be achieved?

Q2.With appropriate scenarios outline the usage of business key and service key And binding key returned by UDDI during publishing of the business and web service for an organization.



Q3.
Consider the XML digital signed document sent from A to B as given below. Outline how the receiver of the document B will validate who has sent it and the integrity of the same.

```
<license>
  <computerName>MYCOMPUTER</computerName>
  <expires>2003-09-31T00:00:00</expires>
  <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>
      <CanonicalizationMethod
        Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" />
      <SignatureMethod
        Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
      <Reference URI="">
        <Transforms>
          <Transform
          Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature" />
        </Transforms>
        <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
        <DigestValue>eU3Par59M28X1c1DNORnhmW0Z2Y=</DigestValue>
      </Reference>
    </SignedInfo>

<SignatureValue>epyuHLJbmyscoVMg2pZZAtZJbBHsZFUCwE4Udv+u3TfiAms2HpLgN3c
L
NtR1xyQpvWt1FKAB/SCk1jr0IaeE7oEjCp2mDOOHhTUTyiv2vMJgCRecC1PLcrmR9ABhqk
      itsjzrCt7V3eF5SpObdUFqcj+n9gjuFnPQt1QeWcvKEcg=</SignatureValue>
  </Signature>
```

</license>

Q4. Outline with clear example the need for XKMS web service.

Q5. From the given HelloService.wsdl document derive the type of the web service, its location, its method and parameters, protocol, and binding.

```
<?xml version="1.0" encoding="UTF-8"?>
<definitions name="HelloService"
   targetNamespace="http://www.ecerami.com/wsdl/HelloService.wsdl"
   xmlns="http://schemas.xmlsoap.org/wsdl/"
   xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
   xmlns:tns="http://www.ecerami.com/wsdl/HelloService.wsdl"
```

```
    xmlns:xsd="http://www.w3.org/2001/XMLSchema">

    <message name="SayHelloRequest">
       <part name="firstName" type="xsd:string"/>
    </message>
    <message name="SayHelloResponse">
       <part name="greeting" type="xsd:string"/>
    </message>

    <portType name="Hello_PortType">
       <operation name="sayHello">
          <input message="tns:SayHelloRequest"/>
          <output message="tns:SayHelloResponse"/>
       </operation>
    </portType>

    <binding name="Hello_Binding" type="tns:Hello_PortType">
       <soap:binding style="rpc"
          transport="http://schemas.xmlsoap.org/soap/http"/>
       <operation name="sayHello">
          <soap:operation soapAction="sayHello"/>
          <input>
             <soap:body

encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
                namespace="urn:examples:helloservice"
                use="encoded"/>
          </input>
          <output>
             <soap:body

encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
                namespace="urn:examples:helloservice"
                use="encoded"/>
          </output>
       </operation>
    </binding>

    <service name="Hello_Service">
       <documentation>WSDL File for HelloService</documentation>
       <port binding="tns:Hello_Binding" name="Hello_Port">
          <soap:address
             location="http://localhost:8080/soap/servlet/rpcrouter"/>
       </port>
    </service>
</definitions>
```

BITS, Pilani-Dubai ,
International Academic city
IV Year Second Semester 2009-10
Degree:B.E.(Hons) Branch:C.S.E

COURSE NO. : CS UC441

Selected topics from computer science

Date:16th Dec 2009 **Total marks=20 (open book) Weightage=20%**

Test2 Open book **Answer all the questions Time- 50 mts**

Text book and class notes are permitted

Q1. I want to host a web service by name weatherforecast.
The web service supports a method by name int Getweather(String city).
It is hosted on a server http://www.xyz.com/. The client needs to give a soap request and get a soap response. We need to use Soap over http protocol.
Derive the weatherforecast.wsdl for the web service.(5M) .
Make any assumption if there is a need.

Q2.Perform XMl digital signing for the following xml document (5M).

```
<?xml versi on=" 1. 0" ?>
<ancientwonders>
 <wonder>Colossus of Rhodes</wonder>
</ancientwonders>
```

Q3. a)What does it mean for a signed document to be verifiable, non-forgible, and non-repudiable?(2.5M)

Q3b).Compare and contrast the TLS and IP layer security.(2.5M)

Q4.a) Consider the CA servers. Suppose a CA goes down? What is the impact on the ability of parties to communicate securely?(2.5M)

b)In public key cryptography if the private key of mine gets compromised what I have to do immediately ? why ? (2.5M)

Q P

BITS, Pilani-Dubai
International Academic city
IVth Year First Semester 2009-2010
Degree:B.E.(Hons) Branch:C.S.E

COURSE NO. : CS C 441 **COURSE TITLE : :Selected topics from computer science (web services and internet based distributed computing**
Date : 1-10-2009

Test1 **Total marks=25 (Closed book) Weightage=25%**
~~Marking and answering schemes~~ Q P.

Q1. Write the XML schema for the following XML document.(6M)

```
<?xml version="1.0" encoding="UTF-8"?>
<contact>
<name>
<given>Joe</given>
<family>John</family>
</name>
<age>30</age>
<address> Main Road</address>
</contact>
```

Q2.

```
<?xml version="1.0" encoding="UTF-8"?>
<BOOK>
<AUTHOR>
<NAME>MURUGAN</NAME>
<COUNTRY>INDIA</COUNTRY>
</AUTHOR>
<TITLE category="Computer science "> Compilers: Principles, Techniques, and
Tools </TITLE>
<PUBLISHER> Addison-Wesley </PUBLISHER>
<YEAR> 1985 </YEAR>
</BOOK>
```

Ignoring end of line characters that get introduced during typing of XMl document, Outline how to parse and get the name and value of the attribute for the element TITLE of the above XML document using DOM parser.
Explain using either java code or pseudo code (6M)

Q3. Considering the above XML document I want to extract and print just the name of the publisher and the year of publication only by parsing using sax parser. Outline how it can be done using java or pseudo code. (6M)

Q4.Outline how confidentiality and integrity can be obtained for communication between two persons Bob and Alice using public key cryptography.(7M)

question paper

BITS,Pilani-Dubai
International academic city
Selected topics from CSE Quiz2
7th Dec 2009 Time:20 mts
Answer all questions all questions carry equal marks
closed book (marks 7)
~~Answering and marking scheme~~

Q1. Can man in the middle attack possible with symmetric cryptography ?
Since the loss of public key and request for the same is the ultimate reason for man in the middle attack it will not happen in symmetric crypto .

Q2.What is the difference between AH and ESP type of IP security ?
Both are part of IP security. Ah type of security ensures that integrity is maintained and proper authentication is done. Security of the message is not maintained.
In ESP type of security integrity and security of the message is maintained.

Q3.

Consider the xml doc as given below:
<xml>
<contact>
<name> Arun</name>
<age> 35</age>
</contact>

In the above XML doc I want to encrypt the name element.
How the result would like?

<xml>
<contact>
<name> Arun</name>

```
<age> 35</age>
<EncryptedData Type='http://www.w3.org/2001/04/xmlenc#Element'
      xmlns='http://www.w3.org/2001/04/xmlenc#'>
        <CipherData><CipherValue>A23B45C56</CipherValue></CipherData>
      </EncryptedData>

</contact
```

Q4.Specify any two important advantages of XMl encryption over conventional encryption?

Although SSL and TSL are good for securing communications across two parties, they are not suitable for multiparty interactions, which is a typical characteristic of XML/Web service interactions. Also, SSL and TSL do not have the capacity to encrypt only specific parts of the document or to encrypt different portions of the document using different keys—which are critical to XML encryption.

Q5 How playback attack between Alice and Bob can be resolved ?

Using non repetable string.(nonce)Suppose Alice wants to access the resource from Bob By telling " I am alice" Bob challenges Alice by sending a non repeatble string which will be encrypted by Alice using the shared symmetric key.Bob will decrypt the same and verify that the request was from alice.

Q6.How key information is sent in XML encryption ?

- <EncryptedKey CarriedKeyName="Muhammad Imran"
  xmlns='http://www.w3.org/2001/04/xmlenc#'>
- <ds:KeyInfo xmlns:ds='http://www.w3.org/2000/09/xmldsig#'>
    <ds:KeyValue>1asd25fsdf2dfdsfsdfds2f1sd23</ds:KeyValue>
    </ds:KeyInfo>
- </EncryptedKey

BITS, Pilani-Dubai

Intternational Academic city, Dubai

IV th Year, FIRST Semester 2009

Degree:B.E.(HONS) Branch:C.S.E

COURSE NO. : CS C441 **COURSE TITLE: Selected topics from computer science (web services and internet based distributed computing)**

Time : 25 mts Date :19--10-2009 Marks: 8 Quiz1 Closed book

Q1.Outline any 2 intranet environtment for performing distributing computing using component architecture

Q2.Enumerate any 2 advantages of component architecture with non component architecture

Q3.Consider a stock quote company located in www.stockquote.com.
They host a web service by name stock. The web service supports a method Getstockprice which accepts stockname as parameter. Write the soap request for the same without name spaces.

Q4.What is the main difference between Document centric and RPc based web services ?

Q5.Why there is a need for WSDL document in web service usage?

Q6.Draw the diagram of SOA module and briefly explain each block in the same.

Q7.Why intranet based distributed computing technologies using components can not be extended for internet based distributed computing ?

Q8. Outline any 2 significances of UDDI registry.