BITS, Pilani-Dubai ,
International Academic city
IV Year First Semester 2012-13

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

COURSE NO. : CS UC441

Date: 31st Dec 2012

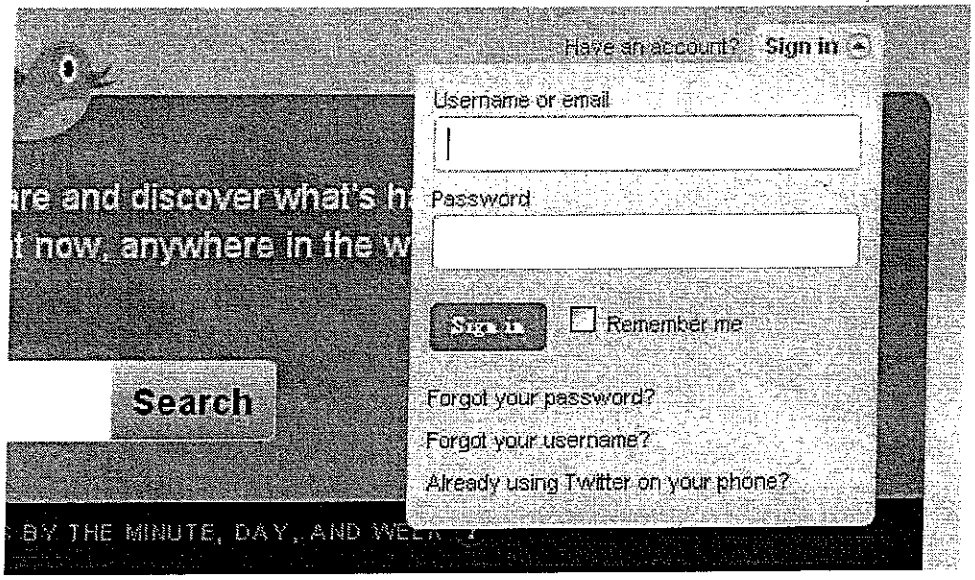
Comprehensive Exam

Selected topics from computer science

Total marks=80 (closed book) Weight age=40%

Answer all the questions Time- 3hrs

Q1.



a)In the above web page I can enter my name and password and get authenticated by submitting the web page to the www.validation.com web server which does the validation using validate.php script. But if I forget to enter the name or age or both then a message alert box has to be displayed in the client side and submission to the server should not be done in this case. Outline a mechanism to achieve the same in the client side ?[4 m]

b)Once he clicks the submit button a remote web application by name validator.php will be invoked and it will give a validation result as simple text as <u>authenticated user</u> or <u>non authenticated user</u> . That info has to be displayed in the client web page. Outline how the above mechanism can be implemented without any hour glass waiting cursor in the browser on clicking the submit button.(8M)

Q2.

```
<MyDocument>

<EncryptedData id="encryptedData1">
```

```
<EncryptionMethod Algorithm=". . ." />
<CipherText>
<CipherValue>. . .</CipherValue>
</CipherText>
<KeyInfo>
<EncryptedKey>
<EncryptionMethod Algorithm=". . ." />
<CipherText>
<CipherValue>. . . </CipherValue>
</CipherText>
<KeyInfo>
<X509Data>
<X509Subject>O=Microsoftcompany,OU=Technology,CN=Jothy
Roesenberg</X509Subject>
</X509Data>
</KeyInfo>
</EncryptedKey>
</KeyInfo>
</EncryptedData>
<Signature>
<SignedInfo>
<CanonicalizationMethod Algorithm=". . ." />
<SignatureMethod Algorithm=". . ." />
<Reference URI="#encryptedData1">
<DigestMethod Algorithm=". . ." />
<DigestValue>. . .</DigestValue>
</Reference>
</SignedInfo>
```

```
<SignatureValue>. . .</SignatureValue>
<KeyInfo>
<X509Data>
<X509Subject>O=IBMCompany,OU=Engineering,CN=David
Remy</X509Subject>
</X509Data>
</KeyInfo>
</Signature>
</MyDocument>
```

a) Comment about the nature of the above doc  sent to a receiver (4M)

b) Outline how the above doc can be successfully decoded at the receiver  ?(8M)

Q3.

```
<definitions name="weatherforecastservice"
   targetNamespace="http://www.examples.com/wsdl/HelloService.wsdl"
   xmlns="http://schemas.xmlsoap.org/wsdl/"
   xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
   xmlns:tns="http://www.examples.com/wsdl/weatherforecast.wsdl"
   xmlns:xsd="http://www.w3.org/2001/XMLSchema">

   <message name="GetTempRequest">
     <part name="city" type="xsd:string"/>
   </message>
   <message name="GettempResponse">
      <part name="temparature" type="xsd:string"/>
   </message>
```

```
  <portType name="Gettemp_PortType">
     <operation name="Gettemp">
        <input message="tns:GettempRequest"/>
        <output message="tns:GettempResponse"/>
     </operation>
  </portType>

 <binding name=”Gettemp_Binding" type="tns: Gettemp_PortType">
 <soap:binding style="rpc"
    transport="http://schemas.xmlsoap.org/soap/http"/>
 <operation name="Gettemp">
    <soap:operation soapAction="Gettemp"/>
    <input>
       <soap:body
          encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
          namespace="urn:examples: weatherforecastservice"
          use="encoded"/>
    </input>
    <output>
       <soap:body
          encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
          namespace="urn:examples: weatherforecastservice"
          use="encoded"/>
   </output>
</operation>
</binding>

<service name=" weatherforecastservice">
```

```
        <documentation>WSDL File for HelloService</documentation>
        <port binding="tns:Gettemp_Binding" name=" Gettemp_PortType ">
           <soap:address
              location="http://www.weatherforecast.com/weatherforecastservice/">
        </port>
    </service>
</definitions>
```

Using the above wsdl doc derive the soap request and response of the `Weatherforecastservice` (6+6)

Q4 . a) Alice and Bob want to send confidential information using public cryptography.

Alice is only familiar with x.509 certificate whereas Bob is used to PGP certificate only.

Outline a mechanism using which they can exchange confidential messages in spite of the above limitation.

b) Further assume that Trudy an intruder has hacked the private key of Alice. Outline a mechanism by which Alice can prevent confidential messages coming to her via public key cryptography?

c)Assume that Alice has got a XML signed message from Bob with the keyinfo specifying the URL of the server from where the certificate of Bob can be downloaded. Assume that Alice does not have the mechanism to process the certificate of Bob and its validity. Suggest an alternative tech by which it can be done.

In all the above cases assume that neither Alice nor Bob has the means to directly communicate with PKI provider

Q5.

```
<?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>
```

Consider the above xml document from Alice to Bob and Trudy. Alice wants to ensure that Trudy should know only the name whereas Bob should know only the CreditCard details. Assume that Alice, Trudy and Bob want to make use of the KDC for secured communication. Outline how it is possible using suitable diagrams.[12M]

## Part-A questions

1.Discuss any 3 important differences between cloud computing and SOA?[4m]

2. what is meant by play back attack in cryptography and how it can be overcome in asymmetric cryptography.[2+2]

3.

```
POST /Stock HTTP/1.1
Host: www.stock.org
Content-Type: application/soap+xml; charset=utf-8 Content-Length: 150

<?xml version="1.0"?>
<soap:Envelope
xmlns:soap="http://www.w3.org/2001/12/soap-envelope"
soap:encodingStyle=http://www.w3.org/2001/12/soap-encoding”>

      <soap:Body xmlns:m="http://www.stock.org/stock">
              <m:GetStockPrice>
                     <m:StockName>IBM</m:StockName>
              </m:GetStockPrice>
      </soap:Body>
</soap:Envelope>
```

A web service is invoked using the above type of soap request.Justify whether the web service is RPC or document centric? Give an example for soap request for a purchase order web service of document centric in nature.[2 +2]

4. How VPN can be built using ESP type of security ? (4)

```
5. <?xml version="1.0" encoding="UTF-8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<xsd:element name="address">
<xsd:complexType>
<xsd:sequence>
<xsd:element ref="name"/>
<xsd:element ref="street"/>
<xsd:element ref="city"/>
<xsd:element ref="state"/>
<xsd:element ref="postal-code"/>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
<xsd:element name="name">
<xsd:complexType>
<xsd:sequence>
<xsd:element ref="title" minOccurs="0"/>
<xsd:element ref="first-Name"/>
<xsd:element ref="last-Name"/>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
<xsd:element name="title" type="xsd:string"/>
<xsd:element name="first-Name" type="xsd:string"/>
<xsd:element name="last-Name" type="xsd:string"/>
```

```
<xsd:element name="street" type="xsd:string"/>
<xsd:element name="city" type="xsd:string"/>
<xsd:element name="state">
<xsd:simpleType>
<xsd:restriction base="xsd:string">
<xsd:length value="2"/>
</xsd:restriction>
</xsd:simpleType>
</xsd:element>
<xsd:element name="postal-code">
<xsd:simpleType>
<xsd:restriction base="xsd:string">
<xsd:pattern value="[0-9]{5}[-][0-9]{4}"/>
</xsd:restriction>
</xsd:simpleType>
</xsd:element>
</xsd:schema>
```

Derive an XML doc that matches the above schema[4M]

Test · 2

BITS,PILANI-DUBAI CAMPUS

INTERNATIONAL ACADEMIC CITY

IV YEAR CS First Semester 2012-13

CS C441 Selected Topics From CS

Test2:20 Marks Date:22-11-2012 Time:50 mts open book

(class notes ,ppt presentation ,text book,reference book are permitted)

Q1.Outline the sequence of events fired by the sax parser when the given xml doc is parsed.[4M]

```
<?xml version="1.0" encoding="UTF-8"?>
<Personnel>

Information about different types of employers

  <Employee type="permanent">
        <Name>Seagull</Name>
        <Id>3674</Id>
        <Age>34</Age>
   </Employee>
  <Employee type="contract">

Employee belongs to india
        <Name>Robin</Name>
        <Id>3675</Id>
        <Age>25</Age>
    </Employee>
  <Employee type="permanent">
        <Name>Crow</Name>
        <Id>3676</Id>
        <Age>28</Age>
    </Employee>
</Personnel>
```

Q2.Suppose Alice and Bob are communicating information using a secured manner. Let Trudy be an intruder. Let them make use of certificates certAlice and CertBob.[1+2+1]

a)How Alice will validate the certificate of Bob?

b) Justify under what circumstances Alice will revoke her certificate.

c) Suppose Alice's certificate has been known to Trudy. Justify whether Alice will revoke her certificate?

Q3.

Given below is the soap request given by a client to credit card validation service.

```
POST  /CCvalidateservice  HTTP/1.1

Host: www.CCvalidator.org

Content-Type: application/soap+xml; charset=utf-8 Content-Length: 150

<?xml version="1.0"?>

<soap:Envelope

xmlns:soap="http://www.w3.org/2001/12/soap-envelope"
soap:encodingStyle=http://www.w3.org/2001/12/soap-encoding”>

   <soap:Body xmlns:m="http://www.stock.org/stock">

         <m:dovalidate>

             <m:CCNumber>2035678654321</m:CCNumber>

         </m:dovalidate>

   </soap:Body>

</soap:Envelope>
```

a)Justify with reasons whether  you can apply  SSL security to protect the Confidentiality of CCNumber?

b)Can you suggest any other better secured mechanism for CCNumber other  than SSL security?

c)Why there is a need for soap client to verify the certificate of server where the web service is hosted once SSL communication is initiated?[1+1+2]

Q4. Suppose Alice and Bob are communicating information. Let Trudy be an intruder.[2+2]

What is meant by IP spoofing attack launched by Trudy? Can you stop that attack using application layer security? If not  justify any other security mechanism that can be used to prevent the attack?

Q5. What is the difference between ESP security in Transport mode and ESP security in Tunnel mode ?[2+2]

How a packet (ESP security in Tunnel mode) received by a router at the receiving end will be handled before the final  IP datagram is passed  to the final destination of a VPN.

Test 1

BITS,PILANI-DUBAI CAMPUS
INTERNATIONAL ACADEMIC CITY
IV YEAR CS First Semester 2012-13
CS C441 Selected Topics From CS
Test1:20 Marks Date:8-10-2012 Time:50 mts Closed book

Q1. Write the XML schema for the following XML document.(4marks)

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

Q2.Justify under what circumstances you will go for RPC web service and Document centric web services with examples.(4M)

Q3.Outline the difficulties you face when you use DCOM and RMI for internet based distributed computing. How the usage of SOAP resolve the above issues? [4M]

Q4.outline how you combine the following XML docs into a single one ?[4M]
In the first doc table indicates html tag whereas in the second doc it represents the physical table.

```
<? xml version="1.0" encoding="UTF-8"?>
<table>
  <tr>
    <td>Apples</td>
    <td>Bananas</td>
  </tr>
</table>
```

```
<? xml version="1.0" encoding="UTF-8"?>
<table>
  <name>African Coffee Table</name>
  <width>80</width>
  <length>120</length>
</table>
```

Q5.what is the difference between a valid and well formed XML docs?[4M]
With the help of simple examples justify when a well formed XML doc becomes invalid?

question paper

QUIZ2 Sel topic
QP

BITS,Pilani-dubai campus

IV th year CS First semester 2012-13

CS C441 Selected topics from CS

Quiz2:closed book  Date:27-12-12 Time 20 mts   Marks:10

1. Specify any two important advantages of XML encryption over  SSL security ?

2.what is meant by password digest authentication in web service request ?

3.what will be the resultant output of the xml doc given below after you encrypt the salary element only

- <Employee>
- <EmployeeID>512-34-4567</EmployeeID>
- <Manager>Fred Jones</Manager>
- <Salary>$50,000</Salary>
- </Employee>

4 .How the receiver of the below document will verify the integrity of the xml doc.

```
    <PurchaseOrderDocument>
    <PurchaseOrder id="po1">
    <SKU>12366</SKU>
    <Quantity>17</SKU>
    </PurchaseOrder>
    <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>
    <Reference URI="#po1" />
    </SignedInfo>
    <SignatureValue>...</SignatureValue>
    <KeyInfo>...</KeyInfo>
    </Signature>
   </purchaseOrder>
</<PurchaseOrderDocument>
```

5.how the receiver of the below document will  decrypt the XML doc given below:

```
 <EncryptedData>
<EncryptionMethod Algorithm=http://www.w3.org/2001/04/xmlenc#aes128-cbc" />
<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmlsig#" />
<EncryptedKey>
<EncryptionMethod Algorithm=http://www.w3.org/2001/04/
xmlenc#rsa-1_5" />
<ds:KeyInfo xmlns:ds=http://www.w3.org/2000/09/xmlsig# />
<ds:X509Data>
<ds:X509SubjectName>
o=MyCompany,ou=Engineering,cn=Dave Remy
</ds:X509SubjectName>
</ds:X509Data>
<ds:/KeyInfo>
<CipherData>
<CipherValue>. . .</CipherValue>
</CipherData>
</EncryptedKey>
</ds:KeyInfo>
<CipherData>
<CipherValue>. . .</CipherValue>
</CipherData>
</EncryptedData>
```

## BITS,Pilani-dubai campus

## IV th year CS First semester 2012-13

## CS C441 Selected topics from CS

## Quiz1:closed book  Date:24-10-12 Time 20 mts   Marks:10

**Only for the first question you are permitted to use altova xml spy editor if you wish.**

```
Q2. POST /Stock HTTP/1.1
Host: www.stock.org
Content-Type: application/soap+xml; charset=utf-8 Content-Length: 150

<?xml version="1.0"?>
<soap:Envelope
xmlns:soap="http://www.w3.org/2001/12/soap-envelope"
soap:encodingStyle=http://www.w3.org/2001/12/soap-encoding”>

     <soap:Body xmlns:m="http://www.stock.org/stock">
              <m:GetStockPrice>
                     <m:StockName>IBM</m:StockName>
              </m:GetStockPrice>
     </soap:Body>
</soap:Envelope>
```

You are given soap request message from a web service client. Justify whether the web service is RPC or documentric centric web service[2M]

Q3.Derive an xml doc which satisfies the schema given below:[2M]

```
?xml version="1.0" encoding="UTF-8"?>
<xs:schema      xmlns:xs="http://www.w3.org/2001/XMLSchema"      elementFormDefault="qualified"
attributeFormDefault="unqualified">
<xs:element name="PurchaseOrder">
<xs:annotation>
```

```
<xs:documentation>To purchase mobiles</xs:documentation>
</xs:annotation>
<xs:complexType>
<xs:sequence>
<xs:element name="Order" minOccurs="2" maxOccurs="2">
<xs:complexType>
<xs:sequence>
<xs:element name="ReplyMail">
<xs:simpleType>
<xs:restriction base="xs:string">
<xs:pattern value="[a-z]{4}[@][a-z]{7}[.][c][o][m]"/>
</xs:restriction>
</xs:simpleType>
</xs:element>
<xs:element name="Qty">
<xs:simpleType>
<xs:restriction base="xs:unsignedInt">
<xs:minInclusive value="20"/>
<xs:maxInclusive value="99"/>
</xs:restriction>
</xs:simpleType>
</xs:element>
<xs:element name="ItemID">
<xs:simpleType>
<xs:restriction base="xs:integer">
<xs:totalDigits value="3"/>
</xs:restriction>
</xs:simpleType>
</xs:element>
</xs:sequence>
</xs:complexType>
</xs:element>
</xs:sequence>
</xs:complexType>
</xs:element>
</xs:schema>
```

Q4.Using pseudo code or java code outline how will you extract the attribute for the XML doc given in question1 using Dom parser assuming that the parser object is already available **as Domparserobj** of type **DocumentBuilder.[2M]**

Q5.suppose I want to create an XML doc like this:[2M]

```
        <?xml version="1.0" encoding="UTF-8"?>
          <Maths>
            <formula> A >B </formula>
            <population>1000</population>
      </Maths>
```

Justify whether it is a well formed XML doc. If not how will you make it well formed.

Q1.Derive an xml schema for the following XML doc. [2M]

```
<?xml version="1.0"?>
<!-- Books written by an author -->
<author>
<name> Lee </name>
<Title country="india">C#</Title>
<Title country="usa">java</Title>
<ISBN>20031</ISBN>
</author>
```

Assume that ISBN can have only 5 digits.