BITS, Pilani-Dubai Campus,
International academic city,Dubai
IVth Year Second semester 2010-11
Degree:B.E.(Hons) Branch:C.S.E

COURSE NO. : CS C441 **Selected topics from computer science**

Test1 Date:25-5-11 **Total marks=80 (closed book) Weightage=40%**

Time:3 hrs **Answer all the questions**

PART-A
(answer all the questions 5 *12=60 M)

Q1.

```
<!-- An author -->
<author>
<name gender = "male">
<first> Art </first>
<last> Gittleman </last>
</name>
<employeeno>236543</employeeno>
</author>
```

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 employee no of the above xml document. 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]

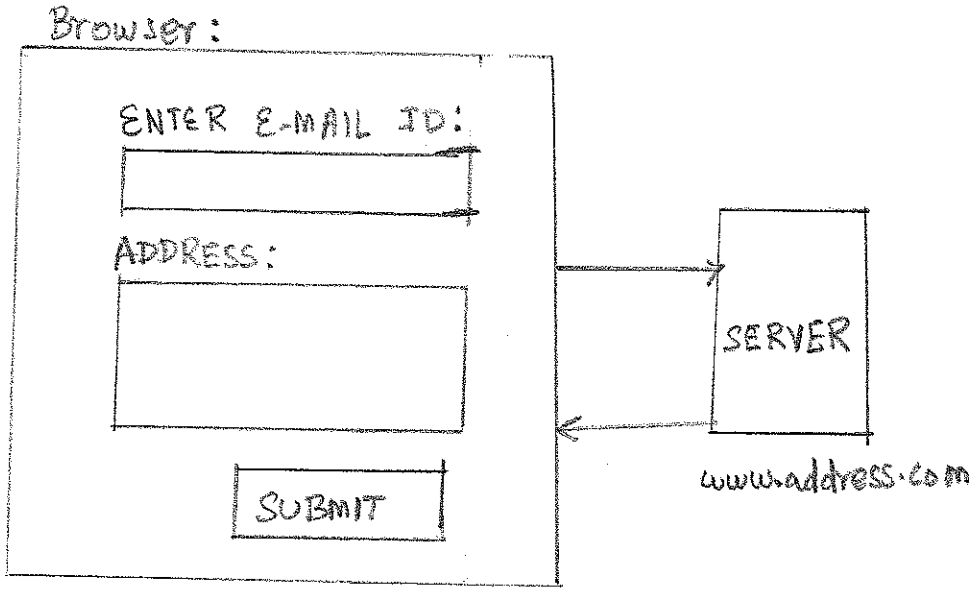
Q2.

```
<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.consider a web form as shown in fig1.



Let the form contains 2 text boxes . Textbox1 is a single string and Textbox2 is a multi line text box. Once the user enters the e-mail ID via Textbox1 and do the submission then the unique address of the person will be returned by the getadrees.php running on the server which can be used to fill the TextBox2.Outline a mechanism to achieve the same without any hourglass waiting cursor when you click the submit button.(12M)

Q4.

```
<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)

Q5.a)Outline the techniques involved during publishing business/web service in the UDDI to enable efficient search of UDDI (4)

b)what is meant by business key,service key and binding key and why they are returned by the UDDI? (4)

c)Outline the need for qualifiers during search of information from UDDI (4)

PART-B

Answer all the questions (5*4=20)

Q1.Briefly explain SSO browser profile in SAML ?

Q2.what is IP spoofing and how it can be avoided using ip security?

Q3.what is meant a client authenticating to a web service and briefly discuss a well known authentication mechanism

Q4.

```
import org.w3c.dom.Document;
import org.w3c.dom.Element;
import org.w3c.dom.NodeList;
import org.w3c.dom.Text;
import javax.xml.parsers.DocumentBuilder;
import javax.xml.parsers.DocumentBuilderFactory;
import java.io.*;
import javax.xml.transform.*;
import javax.xml.transform.dom.*;
import javax.xml.transform.stream.*;
import org.w3c.dom.*;
public class Dom {
 public static void main(String[] args) {
  try {
   DocumentBuilderFactory factory =
            DocumentBuilderFactory.newInstance();
   boolean validate = false;
   factory.setValidating(validate);
   DocumentBuilder builder = factory.newDocumentBuilder();
   Document  dom = builder.newDocument();
  // Document document = builder.parse("D:/authorupdated.xml");
   Element rootEle = dom.createElement("Books");
   dom.appendChild(rootEle);
                Element bookEle = dom.createElement("Book");
                bookEle.setAttribute("Subject","java");
    rootEle.appendChild(bookEle);
                //create author element and author text node and attach it to bookElement
                Element authEle = dom.createElement("Author");
                Text authText = dom.createTextNode("Peterson");
                authEle.appendChild(authText);
                rootEle.appendChild(authEle);

                //create title element and title text node and attach it to bookElement
                Element titleEle = dom.createElement("Title");
                Text titleText = dom.createTextNode("Java Unleashed");
                titleEle.appendChild(titleText);
                rootEle.appendChild(titleEle);

  TransformerFactory transformerFactory = TransformerFactory.newInstance();
```

```
        Transformer transformer = transformerFactory.newTransformer();
        DOMSource source = new DOMSource(dom);
        StreamResult result =  new StreamResult(System.out);
        transformer.transform(source, result);
                        File file = new File("D://output.xml");

        Result result1 = new StreamResult(file);
        transformer.transform(source, result1);
      }
     catch (Exception e) {
       e.printStackTrace();
     }


  }
```

Discuss step by step the actions performed by the above code and final output

Q5.

```
/*
 * To change this template, choose Tools | Templates
 * and open the template in the editor.
 */


/* Uses a SAX parser to identify the parts of an XML
 * file. The user specifies whether to use a validating parser.
 */
import org.xml.sax.Attributes;
import org.xml.sax.helpers.DefaultHandler;
import org.xml.sax.XMLReader;
import javax.xml.parsers.SAXParserFactory;
import javax.xml.parsers.SAXParser;
import org.xml.sax.InputSource;
import java.io.FileReader;

public class Sax extends DefaultHandler {
  private int level = 0;
   private String docName;
   boolean flag= false;

  public void characters(char[] ch, int start, int length){
    String s = new String(ch,start,length);
     while ( flag  )
     {
      System.out.println( s);
      flag=false;
    }

    }
 //
 public void endDocument() {
   System.out.println("End " + docName);
 }
```

```
  public void endElement
      (String uri, String localName, String qName) {

   System.out.println("End element " + localName);
  }
  public void startDocument() {
   System.out.println("Start " + docName);
  }
  public void startElement(String uri, String localName,
                String qName, Attributes attributes){

   //System.out.println("Start element " + localName);
   System.out.println("Start element " + qName);

   if( qName=="first")
   flag =true;
   for (int i = 0; i < attributes.getLength(); i++)
    System.out.println("Attributes "
      + attributes.getLocalName(i) + '' + attributes.getValue(i));
  }
  public static void main(String[] args) {
   Sax sax = new Sax();
   sax.docName ="file///D://authorSimple.xml";
   try {
    SAXParserFactory factory = SAXParserFactory.newInstance();
    boolean validate = false;
    factory.setValidating(validate);
    SAXParser parser = factory.newSAXParser();
    XMLReader reader = parser.getXMLReader();
    reader.setContentHandler(sax);
    reader.parse(new InputSource(new FileReader("D://authorSimple.xml")));
   }catch (Exception e) {
     e.printStackTrace();
   }
  }
}
```

The authorsimple.xml file is given below

```
<?xml version="1.0"?>
<!-- An author -->
<author>
  <name  gender = "male">
    <first> Art </first>
    <last> Gittleman </last>
  </name>
</author>
```

Now discuss about the results of the outcome of the execution of above programme.

Suppose within the while statement of the method public void characters(char[] ch, int start, int length)
if the flag variable is not set to false what will happen ?

BITS, Pilani-Dubai Campus

IV th year Second Semester 2010-2011

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

COURSE TITLE : :Selected topics from computer science

(web services Technology)

COURSE NO. : CS C 441

Date : 8-5-2011

Test2 Time=50 mts **Total marks=20 (open book) Weightage=20% open book**

Q1.outline the difference in providing authentication using embedded SAML assertions and password based digest for authenticating a client to web service. (5M)

Q2. Given the code for digital signing as given below:

```
import java.security.*;
import javax.crypto.*;
public class DigitalSignature {

 public static void main (String[] args) throws Exception {
  String trial1="This is test";
  String trial2="This is    test";
  byte[] plainText = trial1.getBytes("UTF8");
  byte[] plainText2=trial2.getBytes("UTF8");

  MessageDigest messageDigest = MessageDigest.getInstance("MD5");
  System.out.println( "\n" + messageDigest.getProvider().getInfo() );
```

```
messageDigest.update( plainText );
byte[] md = messageDigest.digest();
System.out.println( "\nDigest: " );
System.out.println( new String( md, "UTF8") );

System.out.println( "\nStart generating RSA key" );
KeyPairGenerator keyGen = KeyPairGenerator.getInstance("RSA");
keyGen.initialize(1024);
KeyPair key = keyGen.generateKeyPair();
System.out.println( "Finish generating RSA key" );
Cipher cipher = Cipher.getInstance("RSA/ECB/PKCS1Padding");
System.out.println( "\n" + cipher.getProvider().getInfo() );

System.out.println( "\nStart encryption" );
cipher.init(Cipher.ENCRYPT_MODE, key.getPrivate());
byte[] cipherText = cipher.doFinal(md);
System.out.println( "Finish encryption: of Digest" );
System.out.println( new String(cipherText, "UTF8") );

System.out.println( "\nStart decryption of digest" );
cipher.init(Cipher.DECRYPT_MODE, key.getPublic());
byte[] newMD = cipher.doFinal(cipherText);
System.out.println( "Finish decryption:  of received digest" );
System.out.println( new String(newMD, "UTF8") );
```

```
    System.out.println( "\nStart signature verification of the received message" );
    messageDigest.reset();

    messageDigest.update(plainText2);
    byte[] oldMD = messageDigest.digest();
    int len = newMD.length;
    if (len != oldMD.length) {
     System.exit(1);
    }
    for (int i = 0; i < len; ++i)
     if (oldMD[i] != newMD[i]) {
            System.exit(1);
     }
    System.out.println( "Signature verified" );
  }
}
```

What is the size of the key that is used for digital signing ? (1)

What is the type of algorithm used for encryption ? (1)

How the digest verification takes place ? (2)

Which key is used for signing the digest and why ? (1)

Q3. Given the signed soap request message as given below outline how the integrity of the message can be verified ? (5M)

```
<S:Envelope>
<S:Header>
<wsse:Security>
<wsse:BinarySecurityToken
ValueType="wsse:X509v3"
EncodingType="wsse:Base64Binary"
wsu:Id="X509Token">
FlgEZzCRF1EgILBAgIQEmtJZc0rqrKh5i...
</wsse:BinarySecurityToken>
<ds:Signature>
<ds:SignedInfo>
<ds:CanonicalizationMethod
Algorithm=" http://www.w3.org/2001/10/xml-exc-c14n#" />
<ds:SignatureMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
<ds:Reference URI="#body">
<ds:Transforms>
<ds:Transform
Algorithm=" http://www.w3.org/2001/10/xml-exc-c14n#" />
</ds:Transforms>
<ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
<ds:DigestValue>EULddytSo1...</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>
XLdER8=ErToEb1l/vXcMZNNjPOV...
</ds:SignatureValue>
<ds:KeyInfo>
<wsse:SecurityTokenReference>
<wsse:Reference URI="#X509Token"/>
</wsse:SecurityTokenReference>
</ds:KeyInfo>
</ds:Signature>
</wsse:Security>
</S:Header>
<S:Body wsu:Id="body">
<StatusRequest xmlns="http://www.myCompany.com/Order">
<OrderNumber>1234</OrderNumber>
</StatusRequest>
</S:Body>
</S:Envelope>
```

Q4. Consider Alice and BOB. Both of them want to do secured conservation.

a)Alice wants to have PGP certificate whereas Bob wishes to have X.509 certificate. They want to do secured exchange of confidential files using public key cryptography.(2M)

b)In the mean time Alice finds that its private key got corrupted .(2M)

c) Or Alice finds that its private key got compromised by Trudy. (1M)

Outline a solution about how to tackle the above issues with minimum software overhead in Alice'system and Bob's system

BITS, Pilani-Dubai Campus

IV th year Second Semester 2010-2011

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

COURSE TITLE : :Selected topics from computer science

(web services and Technology)

COURSE NO. : CS C 441 **Date : 20-3-2011**

Total marks=20 (Closed book) Weightage=20% closed book

Test1 Time=50 mts

Answer all the questions

Q1. Outline the need for Digital certificate in a cryptographic system with an example.[2.5+2.5]

Why there is a need for certificate revocation list ?

Q2. I want to parse the below xml doc using sax parser. During parsing I want to print only the content of the **element heading**. Outline a mechanism to achieve the same using java code or pseudo code.[5m]

```
<?xml version="1.0"?>
<note>
  <to>Tove</to>
  <from>Jani</from>
  <heading>Reminder</heading>
  <body>Don't forget me this weekend!</body>
</note>
```

Q3.outline a mechanism by which play back attack can be eliminated in symmetric cryptography and asymmetric cryptography during authentication of Alice to Bob.[5 m]

Q4.Create the following xmL doc using DOM parser using appropriate java code or pseudo code and save it in a file called newdoc.xml ?[5 m]

```
<?xml version="1.0"?>
<note>
  <to>Tove</to>
  <from>Jani</from>
  <heading>Reminder</heading>
  <body>Don't forget me this weekend!</body>
</note>
```

BITS,Pilani-Dubai

International academic city,

IV th CSE second semester 2010-11

CS C441 Selected topics from cse

Quiz 2: Total time:20 mts marks:10 (closed book)

11th april 2011 Answer all the questions

1.what is the need for ESP type of IP security ?(2)

2..How VPN can be built using ESP type of security ? (2)

3. List out the steps involved in decrypting the following XML encrypted doc at the receiving end ? (3)

```
<Employee>
<Name>Dave Remy</Name>
<SocialSecurityNumber>
<EncryptedData id="socsecnum" Type="http://www.w3.org/2000/09/
xmldsig#content">
<KeyInfo>
<KeyName>Jothy Rosenberg</KeyName>
</KeyInfo>
<EncryptionMethod Algorithm=". . ." />
<CipherData><CipherValue>. . .</CipherValue></CipherData>
</EncryptedData>
</SocialSecurityNumber>
<Salary>
<EncryptedData id="salary" Type="http://www.w3.org/2000/09/
xmldsig#content">
<EncryptionMethod Algorithm=". . .">
<CipherData><CipherValue>. . .</CipherValue></CipherData>
</EncryptedData>
</Salary>
<EncryptedKey>
<EncryptionMethod Algorithm=". . ." />
<CipherData>
<CipherValue>. . .</CipherValue>
</CipherData>
<ReferenceList>
<DataReference URI="#socsecnum" />
<DataReference URI="#salary" />
</ReferenceList>
<CarriedKeyName>Jothy Rosenberg</CarriedKeyName>
</EncryptedKey>
</Employee>
```

4. Specify any two important advantages of XML encryption over SSL security ?(1M)

5. Why there is a need for SPI and sequence number for ESP type of security ?(1M)

6. Justify Whether man in the middle attack can happen in symmetric cryptography? (1)

BITS, Pilani-Dubai Campus

IV th year First Semester 2010-2011

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

COURSE TITLE : :Selected topics from computer science

COURSE NO. : CS C 441 **(web services and Technology)**

Quiz1 Time=20 mts **Total marks=10 Weightage=10% closed book Date=7-3-2011**

Answer all the questions

Q1. What is the difference between Entity java bean and stateless session bean under java component architecture?(1 M)

Q2.Derive an XML doc that satisfies the given schema. (2 M)

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema">
<xs:element name="shiporder">
<xs:complexType>
<xs:sequence>
<xs:element name="orderperson" type="xs:string"/>
<xs:element name="shipto">
<xs:complexType>
<xs:sequence>
<xs:element name="name" type="xs:string"/>
<xs:element name="address" type="xs:string"/>
<xs:element name="city" type="xs:string"/>
<xs:element name="country" type="xs:string"/>
</xs:sequence>
</xs:complexType>
```

```
</xs:element>
<xs:element name="item" maxOccurs="unbounded">
<xs:complexType>
<xs:sequence>
<xs:element name="title" type="xs:string"/>
<xs:element name="note" type="xs:string" minOccurs="0"/>
<xs:element name="quantity" type="xs:positiveInteger"/>
<xs:element name="price" type="xs:decimal"/>
</xs:sequence>
</xs:complexType>
</xs:element>
</xs:sequence>
<xs:attribute name="orderid" type="xs:string" use="required"/>
</xs:complexType>
</xs:element>
</xs:schema>
```

Q3. Justify why DCOM and RMI cannot be used for invocation of remote components across the internet ? (1)

Q4.What Is an XSLT processor ? what is the advantage of having XSLT processor on the server side ?(2M)

Q5. Draw and briefly outline what is meant by Study oriented architecture ?(1)

Q6. Give the java based snippets of code for adding an XML element <Country> India</Country>

at the end of the DOM tree of the given XML document.(1M)

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<bookstore>
  <book category="WEB">
   <title lang="en">Learning XML</title>
   <author>Erik T. Ray</author>
   <year>2003</year>
   <price>39.95</price>
 </book>
</bookstore>
```

Q7.Draw the tree view of the xml doc created by DOM parser ignoring the presence of any end of line characters. (2M)

```
<?xml version="1.0" encoding="UTF-8"?>
<dots>
 this is before the first dot
 and it continues on multiple lines
 <dot x="9" y="81" />
 <dot x="11" y="121" />
 <flip>
  flip is on
  <dot x="196" y="14" />
  <dot x="169" y="13" />
 </flip>
 flip is off
 <dot x="12" y="144" />
 <extra>stuff</extra>
 <!-- a final comment -->
</dots>
```