BITS, Pilani-Dubai Campus
IV th year Second Semester 2012-2013

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

Date : 2-6-2013

Time =3hrs

COURSE NO. : BITS C466 Service oriented computing

Comprehensive exam(closed book) Total marks=80 weightage 40% Answer all the question

Part-A (5 *12=60 M)

Q1.consider the XML part of SOAP request message from a web service client to web service. How the web service will decode the soap request message and understand the same.[6 M]

```
<S:Envelope>
<S:Header>
<wsse:Security>
<xenc:EncryptedKey>
<xenc:EncryptionMethod Algorithm="..."/>
<ds:KeyInfo>
<wsse:SecurityTokenReference>
<wsse:KeyIdentifier EncodingType="wsse:Base64Binary"
ValueType="wsse:X509v3">
F2JfLa0GXSq...
</wsse:KeyIdentifier>
</wsse:SecurityTokenReference>
</ds:KeyInfo>
```

```
<xenc:CipherData>
<xenc:CipherValue>...</xenc:CipherValue>
</xenc:CipherData>
<xenc:ReferenceList>
<xenc:DataReference URI="#body"/>
</xenc:ReferenceList>
</xenc:EncryptedKey>
</wsse:Security>
</S:Header>
<S:Body>
<xenc:EncryptedData Id="body">
<xenc:CipherData>
<xenc:CipherValue>...</xenc:CipherValue>
</xenc:CipherData>
</xenc:EncryptedData>
</S:Body>
</S:Envelope>
```

b) consider the XML part of SOAP request message from a web service client to web service. How the web service will verify the integrity of the message.[6M]

```
<S:Envelope>
<S:Header>
<wsse:Security>
```

```
<wsse:BinarySecurityToken
ValueType="wsse:X509v3"
EncodingType="wsse:Base64Binary"
wsu:Id="X509Token">
FIgEZzCRF1EgILBAgIQEmtJZc0rqrKh5i...
</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>
```

Q2 a)

a) Assume that you are authenticating to a web application in a web server using the web form as given below. Let the URL of the web application in the server is http/www.bitsdubai.com/userverification.php

But if I forget to enter the name or age or both and do the submission 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))Assume that the user always remembers to enter a valid e-mail ID and password.Once he clicks the submit button with valid entries in name and password a remote web application by name validator.php (http://www.anyserver.com/validator.php) will be invoked and at the end of verification, it returns http response headers and a html page as

<html><h> you are authenticated <h></html>.

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]

Enter your e-mail ID

Enter password

SUBMIT

b)

Q3.

Buyer is a web service client and known to a Trusted authority and seller is a web service which is also known to a trusted authority. Seller web service is located at http://www.seller.com/purchaseorderhandler But Buyer and seller are not known to each other.Outline step by step how using SAML soap profile a buyer can place a purchase order successfully with the seller web service.[12 M]

Q4. a)Why there is a need for adding category bag for publishing web service provider or web service and what sort of category bags are available for web service provider ?[4M]

b)Assume that a service provider Microsoft has published a stockquote web service that supports soap over http protocol. The provider then wants to modify the protocol for the web service so that now its uses soap over SMTP protocol. Outline the necessary steps to incorporate the new update in UDDI registry.[4M]

c)Assume that a service provider IBM has published a web service by name weatherforecast with proper bindings in UDDI registry. Now he wants to stop hosting that web service and instead of want to host a new web service creditcardvalidator web service. List out the steps needed for carrying out the above changes in UDDI registry. [4M]

Q5.Assume that A(web client) and B (web server) want to communicate securely using SSL protocol. Let A generates a key pair using RSA crypto. Similarly Let B generates a key pair using RSA crypto. A and B do not know how to communicate directly with PKI certificate authority to get certificate. Neither A nor B is capable of processing a certificate and extract the public key.

a) Outline a mechanism which will help A and B to overcome their limitations and do communication using SSL protocol.[6M]
b) One fine day B finds that its private key got compromised. The mechanism you propose in step a) should also help B to tackle the above situation. {3M]
c)Outline briefly about workflow of web services using BPEL. [3M]

Part –B(5 *4 =20 marks)

Q1.

try{

```
    MessageDigest Digestobj = MessageDigest.getInstance("MD5");
    String mystring1 = "This is  a  test";
    byte[] testbytes1= mystring1.getBytes("UTF8");
    Digestobj.update(testbytes1);
    byte[]  Digestout1 = Digestobj.digest();
    String digest1 = new String(Digestout1,"UTF8");
    System.out.println("the  digest from sending end  is "+digest1);

    KeyPairGenerator keyGen = KeyPairGenerator.getInstance("RSA");
    keyGen.initialize(1024);
    KeyPair key = keyGen.generateKeyPair();
    Cipher cipher = Cipher.getInstance("RSA/ECB/PKCS1Padding");
    cipher.init(Cipher.ENCRYPT_MODE, key.getPrivate());
     byte[] cipherText = cipher.doFinal(Digestout1);
    String cipherstring=new String(cipherText,"UTF8");
}

catch(Exception e)
{

}
```

The above code is executed by sender A to send the message and its digital signature to receiver B. Assume that receiver is having access to the keyPairGenerator object mentioned above , using snippets of code outline how the receiver will verify the integrity of the above message.

Q2.using the keytool command briefly outline the things that can be created for cryptography usage.

Q3.

Look carefully the snippets of code as given below.

```
DocumentBuilderFactory factoryobj = DocumentBuilderFactory.newInstance();
   factoryobj.setValidating(false);
   DocumentBuilder builderobj=factoryobj.newDocumentBuilder();
   Document domtreeobj=builderobj.newDocument();
   Element root=domtreeobj.createElement("Book");
   domtreeobj.appendChild(root);
   Element authorobj=domtreeobj.createElement("Author");
   Text authname=domtreeobj.createTextNode("varun");
   authorobj.appendChild(authname);
   root.appendChild(authorobj);
   Element Titleobj=domtreeobj.createElement("Title");
   Text titlevalue=domtreeobj.createTextNode("java");
   Titleobj.appendChild(titlevalue);
   root.appendChild(Titleobj);
```

Now I want to create in-memory view of a new XML document as given below.

```
<?xml>
```

```
<Contact>

<Details>

<name> Arun</name>

<name country="india">varun</name>

<Title>Dr</Title>

<Details>

</contact>
```

Derive the necessary snippets of code for the same with comments.

Q4.outline the similarity between cloud computing and web services and features that are unique only to cloud computing and features that are relevant to web services only.

Q5.
```
import org.xml.sax.Attributes;

import org.xml.sax.helpers.DefaultHandler;


import javax.xml.parsers.SAXParserFactory;

import javax.xml.parsers.SAXParser;


public class Saxparser extends DefaultHandler

//it implies call back methods in Defaulthandler will be

//implemented by the Saxparser

{

   public static void main(String[] args)

   {

    Saxparser parser =new Saxparser();

   SAXParserFactory factoryobj= SAXParserFactory.newInstance();
```

```
factoryobj.setValidating(false);
try
{

  SAXParser parserobj = factoryobj.newSAXParser();
  parserobj.parse("C:\\BlueJ\\contact.xml",parser);
}
catch(Exception e)
{
    System.out.println("error");
}
}//main ends
 public void startDocument() {
  System.out.println("beginning of parsing of xml doc");
}

public void startElement(String uri, String localName,
                String qName, Attributes attributes)
  {

 }// end of method
public void characters(char ch[], int start, int length)
      throws SAXException {
   System.out.println("characters: " +
                        new String(ch, start, length));
}
```

}// end of class

Assume that the above parser is used to parse the XML document given in Question 3.

We want the contents of the element <name> Arun</name> alone to be printed within characters method. Incorporate the necessary snippets of code to achieve the same.

Answering sheet

BITS, Pilani-Dubai Campus
IV th year Second Semester 2012-2013

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

Date : 2-6-2013

Time =3hrs

COURSE NO. : BITS C466 Service oriented computing

Comprehensive exam(closed book) Total marks=80 weightage 40% Answer all the question

Part-A (5 *12=60 M)

Q1.consider the XML part of SOAP request message from a web service client to web service. How the web service will decode the soap request message and understand the same.[6 M]

```
<S:Envelope>
<S:Header>
<wsse:Security>
<xenc:EncryptedKey>
<xenc:EncryptionMethod Algorithm="..."/>
<ds:KeyInfo>
<wsse:SecurityTokenReference>
<wsse:KeyIdentifier EncodingType="wsse:Base64Binary"
ValueType="wsse:X509v3">
F2JfLa0GXSq...
</wsse:KeyIdentifier>
</wsse:SecurityTokenReference>
</ds:KeyInfo>
```

```
<xenc:CipherData>
<xenc:CipherValue>...</xenc:CipherValue>
</xenc:CipherData>
<xenc:ReferenceList>
<xenc:DataReference URI="#body"/>
</xenc:ReferenceList>
</xenc:EncryptedKey>
</wsse:Security>
</S:Header>
<S:Body>
<xenc:EncryptedData Id="body">
<xenc:CipherData>
<xenc:CipherValue>...</xenc:CipherValue>
</xenc:CipherData>
</xenc:EncryptedData>
</S:Body>
</S:Envelope>
```

By looking at the certificate in the KeyInfo, the web service will know that web service client has encrypted the key1 using the public key in the certificate.The key1 is used to encrypt the Body of the message. Using its private key it will decrypt the encrypted key1.using the decrypted key1 it will decrypt the contents of cipherData in Body message wich will eneble the web service to understand the contents of Body.

b) consider the XML part of SOAP request message from a web service client to web service. How the web service will verify the integrity of the message.[6M]

```
<S:Envelope>
<S:Header>
<wsse:Security>
<wsse:BinarySecurityToken
ValueType="wsse:X509v3"
EncodingType="wsse:Base64Binary"
wsu:Id="X509Token">
FIgEZzCRF1EgILBAgIQEmtJZc0rqrKh5i...
</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=ErToEb1I/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>

Using the keyinfo the web service knows the certificate of web service client.

Then using the public key of the certificate contents of the signature value will be decrypted. Then the digest of the Signed Info will be computed. If both the values are equal then the integrity is maintained. Further the digest of the Body of the soap message will be computed and matched with contents of the Digestvalue.If both the steps are successfully completed then the integrity of the body is confirmed.

Q2 a)

a) Assume that you are authenticating to a web application in a web server using the web form as given below. Let the URL of the web application in the server is http/www.bitsdubai.com/userverification.php

But if I forget to enter the name or age or both and do the submission 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]

In the web form I need to handle the onSubmit event using the javascript code as given below:

```
<form name="contact_form" method="post" action= http/www.bitsdubai.com/userverification.php
onSubmit="return validate_form ( );">


function validate_form ( )
{
        valid = true;
    if ( document.contact_form.e_mail.value == "" )
    {
        alert ( "Please fill in the 'e-mail  box." );
        valid = false;
    }
     if ( document.contact_form.password.value == "" )
    {
        alert ( "Please fill in the password." );
        valid = false;
    }
```

b))Once he clicks the submit button with valid entries in name and password a remote web application by name http://www.anyserver.com/validator.php) will be invoked and at the end of verification, it returns http response headers and a html page as

<html><h> you are authenticated <h></html>.

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]

Enter your e-mail ID

Enter password

SUBMIT

b)

```
<form name="contact_form" method="post"  onSubmit="getCustomerInfo().">


<script language="javascript" type="text/javascript">

   function getCustomerInfo() {
     var request = new XMLHttpRequest();
     var email= document.getElementById("e-mail").value;
var password = document.getElementById("Password").value;

     var url = http/www.bitsdubai.com/userverification.php?param1=email &
param2=password;
      request.open("GET", url, true);
      request.onreadystatechange = updatePage;

     request.send(null);

   }
```

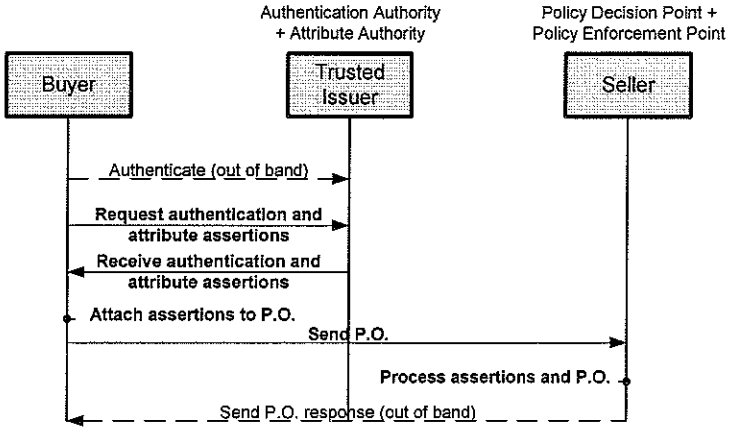
```
function updatePage() {
  if (request.readyState == 4) {
    if (request.status == 200) {
      var response = request.responseText;
       document.innerHTML = response
                } else
      alert("status is " + request.status);
  }
}

</script>
```

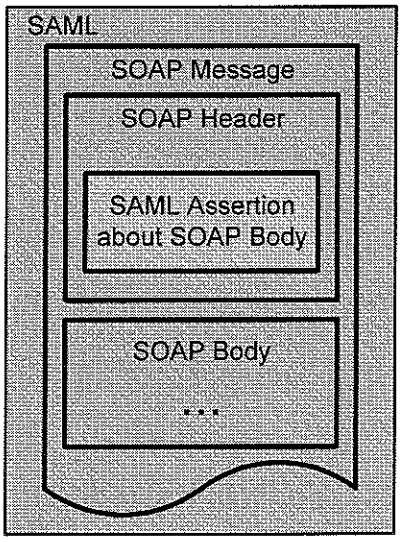
Q3.

Buyer is a web service client and known to a Trusted authority and seller is a web service which is also known to a trusted authority. Seller web service is located at http://www.seller.com/purchaseorderhandler But Buyer and seller are not known to each other.Outline step by step how using SAML soap profile a buyer can place a purchase order successfully with the seller web service.[12 M]

Back office transaction scenario



By contrast, the SOAP profile



Q4. a)Why there is a need for adding category bag for publishing web service provider or web service and what sort of category bags are available for web service provider ?[4M]

To enable search using NAICS category (given a number based on the type of product a company manufacture)

To enable search of a company based on geographical category

By adding category bags we can easily locate the desired company and the desired web service we are interested

b)Assume that a service provider Microsoft has published a stockquote web service that supports soap over http protocol. The provider then wants to modify the protocol for the web service so that now its uses soap over SMTP protocol. Outline the necessary steps to incorporate the new update in UDDI registry.[4M]

delete the existing binding key for soap over http of the web service in the uDDI

publish a new tmodel for the web service whose url points to the new wsdl document of the web service corresponding to soap

c)Assume that a service provider IBM has published a web service by name weatherforecast with proper bindings in UDDI registry. Now he wants to stop hosting that web service and instead of want to host a new web service creditcardvalidator web service. List out the steps needed for carrying out the above changes in UDDI registry. [4M]

Using the deleteservice API and using the business key he can delete the weatherforecast service under the company.Then he should publish the tModel for the creditcard validator web service. Using the tModel key ,using the business key publish the creditcardvalidator service under the business.

Q5.Assume that A(web client) and B (web server) want to communicate securely using SSL protocol. Let A generates a key pair using RSA crypto. Similarly Let B generates a key pair using RSA crypto. A and B do not know how to communicate directly with PKI certificate authority to get certificate. Neither A nor B is capable of processing a certificate and extract the public key.

a) Outline a mechanism which will help A and B to overcome their limitations and do communication using SSL protocol.[6M]
   Let them use XKMS web service and the following methods of the sam.e

- **Register:** Information (credentials) is bound to a key pair through key binding. During registration, either the client provides the public key, along with some proof of possession of the corresponding private key, or the service provider generates the key pair for the client. The service provider

may request more information from the client before it registers the public key (and optionally the private key as well).

-
- **Validate:** This operation does all that locate does, plus more. The locate service finds a key based on the <ds:KeyInfo> element, but does not assure the validity and trustworthiness of the key, cert and binding information. The validate operation not only searches the public key corresponding to the <ds:KeyInfo> element, but also assures that the key binding information that it returns is trustworthy.
-

b) One fine day B finds that its private key got compromised. The mechanism you propose in step a) should also help B to tackle the above situation. {3M]

Revoke: This operation allows clients to destroy the data objects to which a key is bound. For example, an X.509 certificate that's bound to an XKMS key is destroyed when this operation is called

c)Outline briefly about workflow of web services using BPEL. [3M]

BPEL stands for Business Process Execution Language, and comes from a standards consortium consisting of BEA Systems, IBM, and Microsoft, BPEL combines and replaces IBM's WebServices Flow Language (WSFL) and Microsoft's XLANG specification. BPEL provides an "orchestration engine" for describing exchanges of information internally or externally. BPEL deals explicitly with the functional aspects of business processes: control flow (branch, loop, parallel), asynchronous conversations and correlation, long running nested units of work, faults and compensation. BPEL directly addresses these business process challenges: coordinating asynchronous communication between services, correlating message exchanges between parties, implementing parallel processing of activities, manipulating data between partner interactions, supporting long running business transactions and activities, and providing consistent exception handling.

Part –B(5 *4 =20 marks)

Q1.

```
try{
   MessageDigest Digestobj = MessageDigest.getInstance("MD5");
```

```
    String mystring1 = "This is  a  test";
    byte[] testbytes1= mystring1.getBytes("UTF8");
    Digestobj.update(testbytes1);
    byte[]  Digestout1 = Digestobj.digest();
    String digest1 = new String(Digestout1,"UTF8");
    System.out.println("the  digest from sending end  is "+digest1);

    KeyPairGenerator keyGen = KeyPairGenerator.getInstance("RSA");
    keyGen.initialize(1024);
    KeyPair key = keyGen.generateKeyPair();
    Cipher cipher = Cipher.getInstance("RSA/ECB/PKCS1Padding");
    cipher.init(Cipher.ENCRYPT_MODE, key.getPrivate());
    byte[] cipherText = cipher.doFinal(Digestout1);
    String cipherstring=new String(cipherText,"UTF8");
}

catch(Exception e)
{

}
```

The above code is executed by sender A to send the message and its digital signature to receiver B. Assume that receiver is having access to the keyPairGenerator object mentioned above , using snippets of code outline how the receiver will verify the integrity of the above message.

```
Cipher cipher = Cipher.getInstance("RSA/ECB/PKCS1Padding");
   cipher.init(Cipher.DECRCRYPT_MODE, key.getPublic());
```

```
byte[] cipherText = cipher.doFinal(Digestout1);

String cipherstring2=new String(cipherText,"UTF8");
```

//now the receiver should find the digest of received string and compare character by character with that of cipherstring2.If matching is there then integrity is valid.

Q2.using the keytool command briefly outline the things that can be created for cryptography usage.

keytool command in Java is a tool for managing certificates into keyStore and trustStore which is used to store certificate and requires during SSL handshake process. By using **keytool command** you can do many things but some of the most common operation is viewing certificate stored in keystore, importing new certificates into keyStore, delete any certificate from keystore etc. For those who are not familiar keyStore, trustStore and SSL Setup for Java application , Here is a brief overview on **What is a trustStore and keyStore in Java**.
Both trustStore and keyStrore is used to store certificate signed by signer authority or CA (Certificate authority), with keyStore additionally storing personal certificate for client which is used during client authentication on SSL handshake process if its enable. In this article we will see some basic example of keytool command in Java to find how many certificates we have in keyStore , viewing those certificates, adding new certificates and deleting old certificates from keyStore or trustStore in Java.

Q3.

Look carefully the snippets of code as given below.

```
DocumentBuilderFactory factoryobj = DocumentBuilderFactory.newInstance();

factoryobj.setValidating(false);

DocumentBuilder builderobj=factoryobj.newDocumentBuilder();

Document domtreeobj=builderobj.newDocument();

Element root=domtreeobj.createElement("Book");

domtreeobj.appendChild(root);

Element authorobj=domtreeobj.createElement("Author");

Text authname=domtreeobj.createTextNode("varun");
```

```
authorobj.appendChild(authname);
root.appendChild(authorobj);
Element Titleobj=domtreeobj.createElement("Title");
Text titlevalue=domtreeobj.createTextNode("java");
Titleobj.appendChild(titlevalue);
root.appendChild(Titleobj);
```

Now I want to create in-memory view of a new XML document as given below.

```
<?xml>
<Contact>
<Details>
<name> Arun</name>
<name country="india">varun</name>
<Title>Dr</Title>
<Details>
</contact>
```

Derive the necessary snippets of code for the same with comments.

```
DocumentBuilderFactory factoryobj = DocumentBuilderFactory.newInstance();
factoryobj.setValidating(false);
DocumentBuilder builderobj=factoryobj.newDocumentBuilder();
Document domtreeobj=builderobj.newDocument();
Element root=domtreeobj.createElement("Contact");
```

```
domtreeobj.appendChild(root);
Element detail=domtreeobj.createElement("Details");

Element nameobj=domtreeobj.createElement("Name");
Text titlevalue=domtreeobj.createTextNode("Arun");
nameobj.appendChild(titlevalue);
detail.appendChild(nameobj);
Element nameob2j=domtreeobj.createElement("Name");
nameobj2 .setAttribute("Country","India");
Text titlevalue=domtreeobj.createTextNode("Varun");
Nameobj2.appendChild(titlevalue);
Detail.appendChild(Nameobj2);
Element Titleobj=domtreeobj.createElement("Title);
Text titlevalue=domtreeobj.createTextNode("Dr");
Titleobj.appendChild(titlevalue);
detail.appendChild(Titleobj);
root.appendChild(detail);
```

Q4.outline the similarity between cloud computing and web services and features that are unique only to cloud computing and features that are relevant to web services only.

Wrt 1.integration of software components 2.pay as you use nature 3.standard specifications like UDDI,wsdl 4.need for internet

The above comparison need to be made using the above 4 parameters.

Q5. import org.xml.sax.Attributes;

```
import org.xml.sax.helpers.DefaultHandler;

import javax.xml.parsers.SAXParserFactory;
import javax.xml.parsers.SAXParser;

public class Saxparser extends DefaultHandler
//it implies call back methods in Defaulthandler will be
//implemented by the Saxparser
{
   public static void main(String[] args)
   {
    Saxparser parser =new Saxparser();
   SAXParserFactory factoryobj= SAXParserFactory.newInstance();
   factoryobj.setValidating(false);
   try
   {

    SAXParser parserobj = factoryobj.newSAXParser();
    parserobj.parse("C:\\BlueJ\\contact.xml",parser);
   }
   catch(Exception e)
   {
      System.out.println("error");
   }
```

```
}//main ends
    public void startDocument() {
     System.out.println("beginning of parsing of xml doc");
   }

   public void startElement(String uri, String localName,
                 String qName, Attributes attributes)
     {

   }// end of method

}// end of class
```

Assume that the above parser is used to parse the XML document given in Question 3.

We want the contents of the element <name> Arun</name> alone to be printed within

startElement (param1,param2,param3,param4). Incorporate the necessary snippets of code to achieve the same.

Start with a flag which is a global variable and initial value is false.

Within the startElement method first look whether the parameter qName is equal to name. also look whether the attributes object is null.In the above condition set the value of flag equal to true.

Within the characters( ) method of the parser print the contents of the element if the flag is true and then toggles the flag to false.

BITS, Pilani-Dubai Campus
IV th year Second Semester 2012-2013
Degree:B.E.(Hons) Branch:C.S.E

COURSE NO. :BITS C 466 **COURSE TITLE : Service oriented computing**

Date : 25-4-2013

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

Q1.a)Outline the information about the web service(which is needed by a web service client) whose wsdl document is given below.[3]

```
<?xml version="1.0" encoding="UTF-8"?>
<definitions name="ShowInvoiceTotal"
   targetNamespace="http://www.ecerami.com/wsdl/ ShowInvoiceTotal.wsdl"
   xmlns="http://schemas.xmlsoap.org/wsdl/"
   xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
   xmlns:tns="http://www.ecerami.com/wsdl/ShowInvoiceTotal.wsdl"
   xmlns:xsd="http://www.w3.org/2001/XMLSchema">

   <message name="ShowInvoiceTotalRequest">
      <part name="Invoice" type="xsd:Integer"/>
   </message>
   <message name="SHowIayHelloResponse">
      <part name="Invoicetotal" type="xsd:string"/>
   </message>

   <portType name="ShowInvoice_PortType">
      <operation name="GetInvoiceTotal">
         <input message="tns: ShowInvoiceTotalRequest"/>
         <output message="tns: ShowInvoiceTotalResponse"/>
      </operation>
   </portType>

   <binding name=" ShowInvoice_Binding" type="tns:ShowInvoice_PortType">
      <soap:binding style="rpc"
         transport="http://schemas.xmlsoap.org/soap/http"/>
      <operation name="GetInvoiceTotal">
         <soap:operation soapAction="GetInvoiceTotal"/>
         <input>
            <soap:body
               encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
               namespace="urn:examples:ShowInvoiceTotal"
               use="encoded"/>
         </input>
         <output>
            <soap:body
               encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
               namespace="urn:examples:ShowInvoiceTotal"
               use="encoded"/>
         </output>
      </operation>
   </binding>
```

```
   <service name="ShowInvoiceTotal_Service">
      <documentation>WSDL File for show invoice total Service</documentation>
      <port binding="tns:ShowInvoice_Binding" name="ShowInvoice_Port">
         <soap:address
            location="http://localhost:8080/ShowInvoiceTotal"/>
      </port>
   </service>
</definitions>
```

b)Derive the soap request for the above web service[3]

Q2. <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>

Outline how the receiver of the above xml document can decrypt and get the non encrypted XML document.{4M]

Q3.Assume that Alice, Bob and Trudy are in the internet When Alice,s system is off Trudy does IP spoofing and sends packets to Bob .Justify What sort of security is needed to eliminate the attack?[3]

Assume A and B are sending packets to C via internet using IP security. In the above cases why there is a need for security parameter index in IP security enabled packets?[2m]

Q4.a)Consider 3 entities A,B are Communicating across the internet. Let B is the server and A authenticates itself using the its certificate and get the desired info from B. Suppose C is an intruder and he steals the certificate of A and send it to B. Outline an mechanism using which B can identify the above attack?[3M]

b)Justify whether man in the middle attack happen in symmetric cryptography.[2M]

Test - 2 Answer

BITS, Pilani-Dubai Campus
IV th year Second Semester 2012-2013
Degree:B.E.(Hons) Branch:C.S.E

COURSE NO. :BITS C 466 **COURSE TITLE : Service oriented computing**

Date : 25-4-2013

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

Answering scheme

Q1.a)Outline the information about the web service(which is needed by a web service client) whose wsdl document is given below.[3]

```
<?xml version="1.0" encoding="UTF-8"?>
<definitions name="ShowInvoiceTotal"
   targetNamespace="http://www.ecerami.com/wsdl/ ShowInvoiceTotal.wsdl"
   xmlns="http://schemas.xmlsoap.org/wsdl/"
   xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
   xmlns:tns="http://www.ecerami.com/wsdl/ShowInvoiceTotal.wsdl"
   xmlns:xsd="http://www.w3.org/2001/XMLSchema">

   <message name="ShowInvoiceTotalRequest">
      <part name="Invoice" type="xsd:Integer"/>
   </message>
   <message name="SHowIayHelloResponse">
      <part name="Invoicetotal" type="xsd:string"/>
   </message>

   <portType name="ShowInvoice_PortType">
      <operation name="GetInvoiceTotal">
         <input message="tns: ShowInvoiceTotalRequest"/>
         <output message="tns: ShowInvoiceTotalResponse"/>
      </operation>
   </portType>

   <binding name=" ShowInvoice_Binding" type="tns:ShowInvoice_PortType">
      <soap:binding style="rpc"
         transport="http://schemas.xmlsoap.org/soap/http"/>
      <operation name="GetInvoiceTotal">
         <soap:operation soapAction="GetInvoiceTotal"/>
         <input>
            <soap:body
               encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
               namespace="urn:examples:ShowInvoiceTotal"
               use="encoded"/>
         </input>
         <output>
            <soap:body
               encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
               namespace="urn:examples:ShowInvoiceTotal"
               use="encoded"/>
         </output>
      </operation>
   </binding>
```

```
   <service name="ShowInvoiceTotal_Service">
      <documentation>WSDL File for show invoice total Service</documentation>
      <port binding="tns:ShowInvoice_Binding" name="ShowInvoice_Port">
         <soap:address
            location="http://localhost:8080/ShowInvoiceTotal"/>
      </port>
   </service>
</definitions>
```

Parameter of web service	values
Method name	String GetInvoiceTotal(int invoice)
Protocol	Soap over http
Type	RPC and Request/Response
URL of web service	http://localhost:8080/ShowInvoiceTotal

b)Derive the soap request for the above web service[3]

```
POST /ShowInvoiceTotal
Host: localhost:8080
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="urn:examples:ShowInvoiceTotal" >
        <m: GetInvoiceTotal>
            <m:invoice>200</m:invoice>
        </m: GetInvoiceTotal>
   </soap:Body>
</soap:Envelope>
```

Q2. <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>
```

Outline how the receiver of the above xml document can decrypt and get the non encrypted XML document.{4M]

By looking at the CarriedKeyName the receiver will know that symmetric key that is used for encrypting the XML elements is itself encrypted using its certificate. The receiver using the matched private key will decrypt the symmetric key.Then it will decrypt the cipher data present within EncryptedData elements using the symmetric key and get the original non encrypted XML elements.

Q3.Assume that Alice, Bob and Trudy are in the internet When Alice,s system is off Trudy does IP spoofing and sends packets to Bob .Justify What sort of security is needed to eliminate the attack?[3]
We need security at IP level either AH type of security or ESP type of security.
Since using application layer security or SSL we can't make out Ip spoofing.
Assume A and B are sending packets to C via internet using IP security. In the above cases why there is a need for security parameter index in IP security enabled packets?[2m]

SPI is unique number which is included in a security association between A and B.
All the packets which are part of the above SA will have the SPI header. Using that B will refer to a row of database information which will tell what sort of IP security between A to B (AH or ESP),the digest algorithm, the encryption algorithm, size of key and everything using which B can verify the integrity and decrypt the packet.

Q4.a)Consider 3 entities A,B are Communicating across the internet. Let B is the server and A authenticates itself using the its certificate and get the desired info from B.

Suppose C is an intruder and he steals the certificate of A and send it to B.
Outline an mechanism using which B can identify the above attack?[3M]
Then the server has to send a nonce ask the C to encrypt it using the private key which matches the certificate of A. since C does not have the same he will fail and thus B can know that C is an intruder.

b)Justify whether man in the middle attack happen in symmetric cryptography.[2M]

Man in the middle attack happens only when A and B communicate using asymmetric crypto and one of the parties ask other to send its public key over the internet. In symmetric crypto graphy A will not ask B to send the symmetric key and thus the man in middle attack will not happen in symmetric cryptography.

BITS, Pilani-Dubai Campus
IV th year Second Semester 2012-2013

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

COURSE TITLE : Service oriented computing

COURSE NO. : BITS C466 **Date : 7-3-2013**

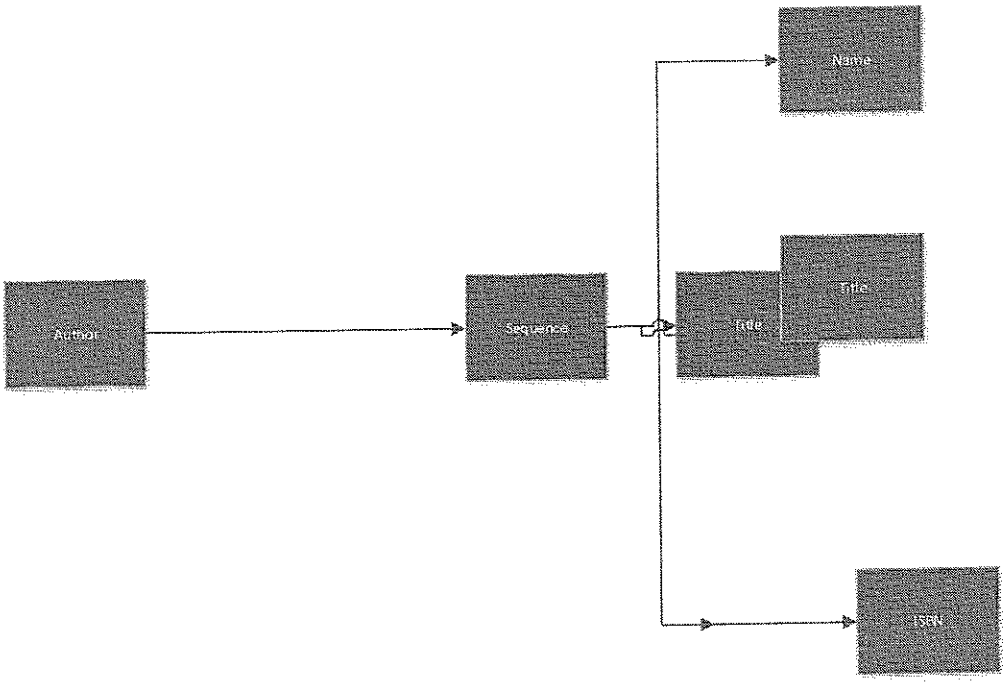
Test1 Time=50 mts **Total marks=20 (Closed book) Weightage=20% closed book**

Q1.Derive an XML doc that satisfies the schema given below?[5m]

```
?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>
```

Q2.In the diagram author,name,Title are simple strings. But ISBN is 5 digit integer.Derive the schmea for the above xml document.[5m]



Q3.Let IBM hosts a web service by name stock quote web service. With appropriate diagram outline how a client discovers the above web service and generate appropriate soap request for invoking the web service and interpret the soap response with minimal overhead in client code. [5m]

Q4.using pseudo code outline how will you parse the given XML document using DOM parser and get the attribute of the element city.[3m]

```
<?xml version="1.0" encoding="UTF-8"?>
<country >
        <state>
                <city Location ="USA">NY</city>
                <language>Eng</language>
                <population>1000</population>
        </state>
        </country>
```

Q5.Outline the limitations of protocols DCOM and RMI when you try to use them for internet based distributed computing of components.[2m]

Answer key Scheme

BITS, Pilani-Dubai Campus
IV th year Second Semester 2012-2013

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

COURSE TITLE : Service oriented computing

COURSE NO. : BITS C466 **Date : 7-3-2013**

Answer

Test1 Time=50 mts **Total marks=20 (Closed book) Weightage=20% closed book**

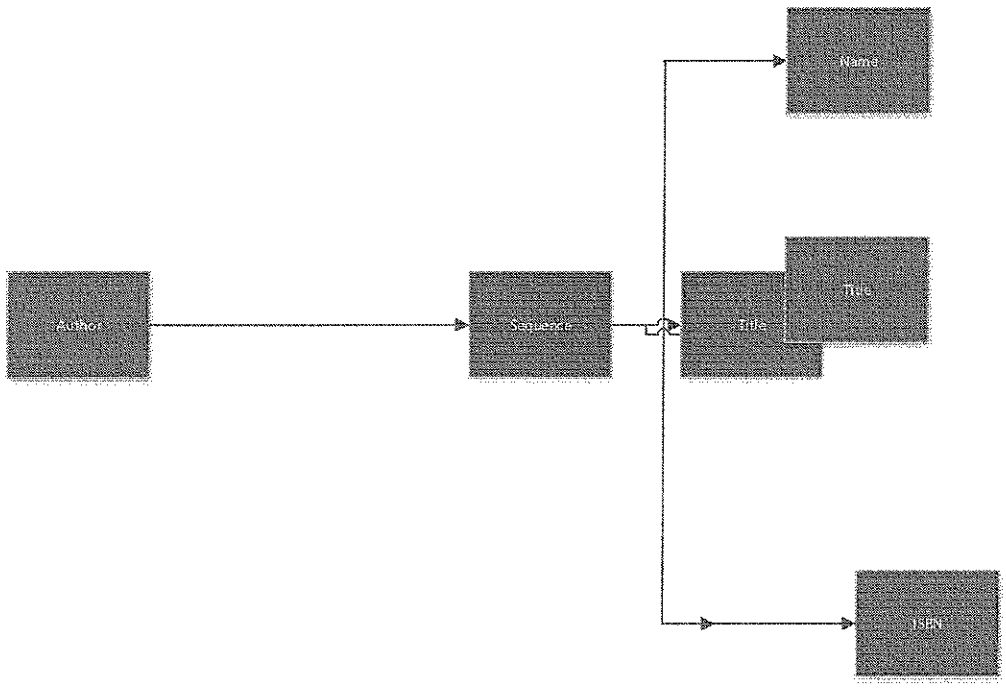
Q1.Derive an XML doc that satisfies the schema given below?[5m]

```
?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>
```

```
?xml version="1.0" encoding="UTF-8"?>
<PurchaseOrder xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="file:///C:/Users/Vadivel/Documents/Altova/XMLSpy2011/Examples/P
urchaseOrder_sep_2012.xsd">
        <Order>
                <ReplyMail>vadi@hotmail.com</ReplyMail>
                <Qty>33</Qty>
                <ItemID>456</ItemID>
        </Order>
        <Order>
                <ReplyMail>mani@hotmail.com</ReplyMail>
                <Qty>22</Qty>
                <ItemID>789</ItemID>
        </Order>
                                        </PurchaseOrder>
```

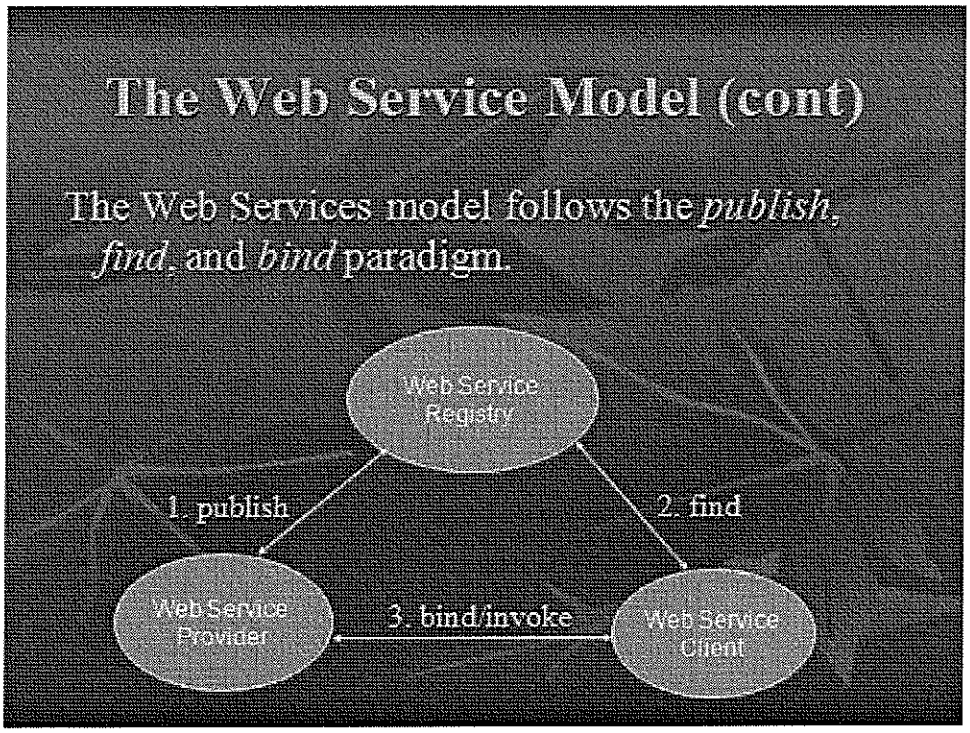
Q2.In the XML tree diagram diagram name,Title are simple strings. But ISBN is 5 digit integer.Derive the schmea for the above xml document.[5m]




```
<xs:element name="author">
        <xs:annotation>
                <xs:documentation>Comment describing your root element</xs:documentation>
        </xs:annotation>
        <xs:complexType>
```

```
                <xs:sequence>
                        <xs:element name="Name" type="xs:string"/>
                        <xs:element name="Title" minOccurs="2" maxOccurs="2">
                                <xs:complexType>
                                        <xs:simpleContent>
                                                <xs:extension base="xs:string">
                                                        <xs:attribute name="Country"
type="xs:string"/>
                                                </xs:extension>
                                        </xs:simpleContent>
                                </xs:complexType>
                        </xs:element>
                        <xs:element name="ISBN">
                                <xs:simpleType>
                                        <xs:restriction base="xs:integer">
                                                <xs:totalDigits value="5"/>
                                        </xs:restriction>
                                </xs:simpleType>
                        </xs:element>
                </xs:sequence>
        </xs:complexType>
</xs:element>
```

Q3.Let IBM hosts a web service by name stock quote web service. With appropriate diagram outline how a client discovers the above web service and generate appropriate soap request for invoking the web service and interpret the soap response with minimal overhead in client code. [5m]



IBM(web service provider) has to publish the web service in UDDI registry so that it can be searched and located by any client across the internet.IBM also has to maintain a copy of stockquote.wsdl doc and info about the same also has to be published in UDDI. Client after finding the IBM service in UDDI then

will look and download the wsdl document. From the wsdl document it will generate a proxy which will be stored in the client machine. The client will invoke the method of proxystockquote locally which will generate soap request to a remote web service. Similarly when the soap response comes from remote client the proxy will remove the result from the soap response and return the same to the soap client

Q4.using pseudo code outline how will you parse the given XML document using DOM parser and get the attribute of the element city.[3m]

```
<?xml version="1.0" encoding="UTF-8"?>
<country >
        <state>
                <city Location ="USA">NY</city>
                <language>Eng</language>
                <population>1000</population>
        </state>
        </country>
```

Create a DOM parser facory

```
import javax.xml.parsers.DocumentBuilder;

import javax.xml.parsers.DocumentBuilderFactory;

import java.io.File;

import org.w3c.dom.Document;

public class OrderProcessor {

public static void main (String args[]) {

File docFile = new File("countrylocation.xml");

Document doc = null;

try {

DocumentBuilderFactory dbf = DocumentBuilderFactory.newInstance();

DocumentBuilder db = dbf.newDocumentBuilder();

doc = db.parse(docFile);

//STEP 1: Get the root element

Element root = doc.getDocumentElement();

System.out.println("The root element is " + root.getNodeName());

//STEP 2: Get the child
```

```
Element state = root.getFirstChild();

Element city =state.getFirstChild();

NamedNodeMap startAttr = city.getAttributes();

for (int i = 0;

i < startAttr.getLength();

i++) {

Node attr = startAttr.item(i);

System.out.println(" Attribute: "+ attr.getNodeName()

+" = "+attr.getNodeValue());



} catch (Exception e) {

System.out.print("Problem parsing the file: "+e.getMessage());

}

}

}
```

Q5.Outline the limitations of protocols DCOM and RMI when you try to use them for internet based distributed computing of components.[2m]

Development of DCOM apps strictly bound to Windows Operating system.

Development of RMI used by EJBS bound to Java programming language

DCOM and RMI use non standard ports and can not navigate through the firewalls which will allow only port 80 communication.

Qu's. 2

BITS, Pilani-Dubai Campus
IV th year Second Semester 2012-2013

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

COURSE TITLE : Service oriented computing

(web services and Technology)

COURSE NO. :BITS C 466 **Date : 28-3-2013**

Total marks=6 (Closed book) Weightage=10% closed book

Quiz2 Time=20 mts

Q1.How password digest authentication in soap request prevents play back attack? (1 M)

Q2.How the receiver of the following message can verify the integrity of the XML? (1M)

```
<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>
</PurchaseorderDocument>
```

Q3.what is meant SSO using browser profile in SAML?(1M)

Q4.what is meant by back office transaction scenario using soap profile?(1M)

Q5.why there is a need for canonicalization method in XML digital signature ?(1M)

Q6.what is the difference between attribute assertion and authentication assertion in SAML ?

BITS, Pilani-Dubai Campus
IV th year Second Semester 2012-2013

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

COURSE TITLE : Service oriented computing

(web services and Technology)

COURSE NO. :BITS C 466 **Date : 28-3-2013**

Answering and marking scheme

Total marks=6 (Closed book) Weightage=10% closed book

Quiz2 Time=20 mts

Q1.How password digest authentication in soap request prevents play back attack? (1 M)
For password digest authentication the shared password between a and B, Random nonce and date & time at which message is sent all are used to form the combined digest.Here the nonce and date&time vary for every message and hence replay attack can not be possible in the above case.
Q2.How the receiver of the following message can verify the integrity of the XML? (1M)

```
<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>
</PurchaseorderDocument>
```

First the receiver will decrypt the signature value using its private key.then the entire purchaseorder element along with its children will be embedded within SignedInfo element and the digest of sigendInfo will be found out. If the decrypted signaturevalue matches with the digest of SignedInfo then that indicates no integrity violation.

Q3.what is meant SSO using browser profile in SAML?(1M)

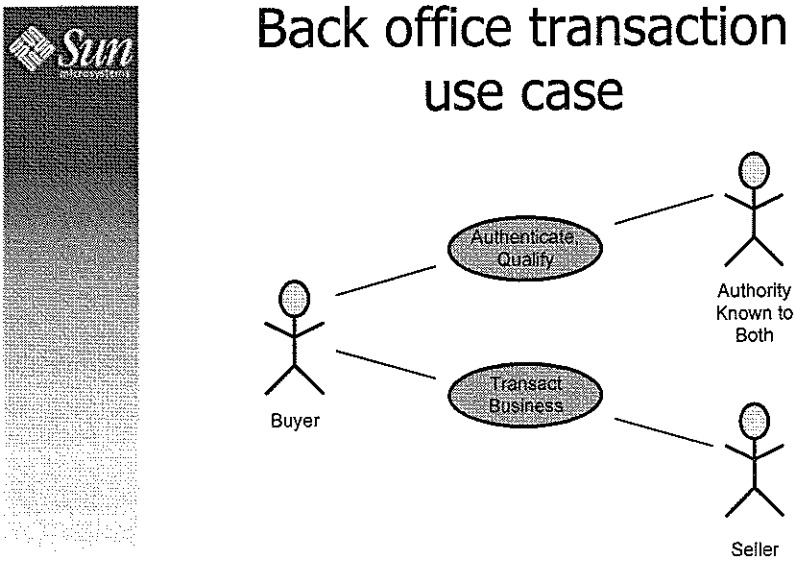
Steps:

1. Web user authenticates to the source Web site.
2. Web user uses a secured resource at the destination Web site.

3. This use case has specific **push** and **pull** scenarios.

There is no need for any fresh authentication at the destination web site.

Q4.what is meant by back office transaction scenario using soap profile?(1M)



Q5.why there is a need for canonicalization method in XML digital signature ?(1M)

The canonicalization method ensures that 2 XML docs that carry the same information but created under different OS get ride of all wanted characters like carriage return,white space (that are specific to an OS) before we find the digest of the any of the above document.

Q6.what is the difference between attribute assertion and authentication assertion in SAML ?

- An attribute assertion issuing authority asserts that:
  - subject S
  - is associated with attributes A, B, ...
  - with values "a", "b", "c"...
- An authentication assertion issuing authority asserts that:
  - subject S
  - was authenticated by means M

- at time T

BITS, Pilani-Dubai Campus
IV th year Second Semester 2012-2013

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

COURSE TITLE : Service oriented computing

(web services and Technology)

COURSE NO. :BITS C 466 **Date : 28-3-2013**

Quiz1 Time=20 mts **Total marks=10 (Closed book) Weightage=10% closed book**

Answer all the questions

Q1.specify any 2 important advantages of DOM parser over sax parser?

Q2. For the following xml document list out the events fired by SAX parser

```
<?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>
```

Q3. Draw the tree structure a DOM parser will create for the above XML document

Q4.Consider the snippets of code for building a DOM parser. I want to create a XML Document tree

Which follows the tree structure of XML doc given below. Derive the pseudo code or java code that needs to be added for the same.

```
<?xml>

<Books>

<Book Subject ="java">java related</Book>

<Author>Tom</Author>

</Books>
```

```
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();

    Element rootEle = dom.createElement("Books");

   dom.appendChild(rootEle);

------------------------------------







}
```

Q5. Suppose N people want to communicate with each of the $N-1$ other people using symmetric key encryption. All communication between any to people, i and j, is visible to all other people, and no other person should be able to decode their communication. How many keys are required in the system as a whole? Now suppose that public key encryption is used. How many keys are required in this case?

BITS, Pilani-Dubai Campus
IV th year Second Semester 2012-2013

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

COURSE TITLE : Service oriented computing

(web services and Technology)

COURSE NO. :BITS C 466

Date : 28-3-2013

Answering Scheme

Total marks=10 (Closed book) Weightage=10% closed book

Quiz1 Time=20 mts

Answer all the questions

Q1.specify any 2 important advantages of DOM parser over sax parser?

1.Edit an XML document

2.create an xml document from scratch

3.Using in memory view of XML document we can traverse the tree using various techniques

Q2. For the following xml document list out the events fired by SAX parser

```
<?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>
```

```
startDocument
startElement: dots (0 attributes)
characters:   this is before the first dot
  and it continues on multiple lines
startElement: dot (2 attributes)
endElement:   dot
startElement: dot (2 attributes)
endElement:   dot
startElement: flip (0 attributes)
characters:   flip is on
startElement: dot (2 attributes)
endElement:   dot
startElement: dot (2 attributes)
endElement:   dot
endElement:   flip
characters:   flip is off
startElement: dot (2 attributes)
endElement:   dot
```

startElement: extra (0 attributes)

characters: stuff

endElement: extra

endElement: dots

endDocument

Q3. Draw the tree structure a DOM parser will create for the above XML document

```
Document
+---Element <dots>
  +---Text "this is before the first dot
  |  and it continues on multiple lines"
  +---Element <dot>
  +---Text ""
  +---Element <dot>
  +---Text ""
  +---Element <flip>
  |  +---Text "flip is on"
  |  +---Element <dot>
  |  +---Text ""
  |  +---Element <dot>
  |  +---Text ""
  +---Text "flip is off"
  +---Element <dot>
  +---Text ""
```

```
+---Element <extra>
|  +---Text "stuff"
+---Text ""
+---Comment "a final comment"
+---Text ""
```

Q4.Consider the snippets of code for building a DOM parser. I want to create a XML Document tree Which follows the tree structure of XML doc given below. Derive the pseudo code or java code that needs to be added for the same.

```
<?xml>
<Books>
<Book Subject ="java">java related</Book>
<Author>Tom</Author>
</Books>
```

```
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();
    Element rootEle = dom.createElement("Books");
   dom.appendChild(rootEle);
```

```
Element bookEle = dom.createElement("Book");

    bookEle.setAttribute("Subject","java");

    Text authText = dom.createTextNode("java related");

    bookEle.appendChild(authText);

    rootEle.appendChild(bookEle);

    //create author element and author text node and attach it to bookElement

    Element authEle = dom.createElement("Author");

    Text authText1 = dom.createTextNode("Tom");

    authEle.appendChild(authText1);

    rootEle.appendChild(authEle);



}
```

Q5. Suppose *N* people want to communicate with each of the *N-1* other people using symmetric key encryption. All communication between any to people, *i* and *j*, is visible to all other people, and no other person should be able to decode their communication. How many keys are required in the system as a whole? Now suppose that public key encryption is used. How many keys are required in this case?

If each user wants to communicate with N other users, then each pair of users must have a shared symmetric key. There are N*(N-1)/2 such pairs and thus there are N*(N-1)/2 keys. With a public key system, each user has a public key which is known to all, and a private key (which is secret and only known by the user). There are thus 2N keys in the public key system.