

**BITS, Pilani-Dubai Campus,
International academic city, Dubai
IVth Year SECOND Semester 2008-09
Degree: B.E.(Hons) Branch: C.S.E
COURSE NO. : CS C441**

Selected topics from computer science

Date: 24-5-09

Total marks=60 (closed book) Weightage=40%

Time: 3 hrs

Answer all the questions

Part-A (answer all the questions 5*2=10 M)

Q1. Outline briefly the need for xml schema in enterprise applications ?

Q2. Outline briefly the ESP based IP security.

Q3. Why there is a need for certificate revocation in PKI ?

Q4. What are the advantages of xml encryption compared to conventional encryption ?

Q5. Outline the differences between ebxml and web service.

Part-B (answer all the questions 5*10=50M)

Q1. I want to develop a web enabled application which displays in a form the EmployeeID , shipping address and order for books . The user will enter the employee code and then enter the order for books. By that time your browser should contact the server and get the shipping address for the employee ID. On submitting the form to the server it should deliver the books to the shipping address. Outline how the above application can be developed ? (10M)

The above thing can be implemented using Ajax. Let the user browse to the URL for the book shopping web site. Let the book shopping site display the form for entering employeeID , shipping address and order for books. Let the user enter the employeeID. Now as soon as the user enters the employee ID invocation then a java script method will be invoked.

Within the method an XMLHttpRequest object will be created. Using that object a connection will be made to the server side application passing the employee ID as the parameter. The server will return an XMLHttpRequest response object.

Q2. The wsdl document for a web service is given below. Now form an appropriate soap request and response for the web service. (5+5)

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

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

```

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

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

<binding name="Hello_Binding" type="tns:Hello_PortType">
  <soap:binding style="rpc"
    transport="http://schemas.xmlsoap.org/soap/http"/>
  <operation name="sayHello">
    <soap:operation soapAction="sayHello"/>
    <input>
      <soap:body
        encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
        namespace="urn:examples:helloservice"
        use="encoded"/>
    </input>
    <output>
      <soap:body
        encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
        namespace="urn:examples:helloservice"
        use="encoded"/>
    </output>
  </operation>
</binding>

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

```

Q3. a) I want to publish an online catalogue web service under the business Microsoft. Under the NAICS category the business has been assigned a number 203022 and grouped under software products. List out the steps involved in publishing the above information in UDDI registry. (7M)

b) Suppose later if we want to change the binding of the web service. How it can be done? (3M)

Q4. Let an employee belongs to www.sun.com. Now let the www.infosysis.com/sunemployees/providentfund.html provides updating provident fund facilities for employess of sun microsystem. Now an employee of sun by doing single sign on at www.sun.com he want to access and update his provident fund facilities at infosysis.com. Outline how using SSO pull using browser profile in SAML this can be done. Make any necessary valid assumptions if needed. (10M)

Q5.a) Outline the merits of xml digital signing compared to conventional digital signing.(3M)

b) Consider an XML document

```
<?xml version="1.0" encoding="UTF-8"?>
<PurchaseOrder>
  <Item number="130046593231">
    <Description>Video Game</Description>
    <Price>10.29</Price>
  </Item>
  <Buyer id="8492340">
    <Name>My Name</Name>
    <Address>
      <Street>One Network Drive</Street>
      <Town>Burlington</Town>
      <State>MA</State>
      <Country>United States</Country>
      <PostalCode>01803</PostalCode>
    </Address>
  </Buyer>
</PurchaseOrder>
```

Outline how xml digital signature is done for the above document.(7M)

BITS, Pilani-Dubai,Campus

Academic city,Dubai

IV th Year Second Semester 2009

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

COURSE NO. : CS C441

**COURSE TITLE: Selected topics from computer science
(web services and internet based distributed computing)**

Time :50 mts

Date :19-4-2009

Marks: 20 Test2 open book

Q1.Consider a KDC and a Certificate Authority servers. Suppose a KDC goes down. What is the impact on ability of parties to communicate securely. That is who can and can not communicate. Justify. Suppose now that a CA goes down. What is the impact of the failure? (2.5+2.5M).

Q2.

```
<?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>
```

Consider the above xml document. I want to get the attributes of Arrow marked dot element alone using sax parser. Using pseudo code explain how it can be done.[5m]

Q3. `<?xml version='1.0' ?>`
`<<SecureCommunicationDemonstration>`
`<Order>`
`<Item>book</Item>`
`<Id>123-958-74598</Id>`
`<Quantity>12</Quantity>`
`<CardName>Visa</CardName>`
`<ExpDate>10-10-2005</ExpDate>`
`<EncryptedData Type='http://www.w3.org/2001/04/xmlenc#Element'`
`xmlns='http://www.w3.org/2001/04/xmlenc#'`
`<EncryptionMethod Algorithm='http://www.w3.org/2001/04/xmlenc#triplede-`
`cbc' />`
`<ds:KeyInfo xmlns:ds='http://www.w3.org/2000/09/xmldsig#'`
`<ds:KeyName>Imran ali</ds:KeyName>`
`</ds:KeyInfo>`
`<CipherData>`
`<CipherValue>A23B45C564587</CipherValue>`
`</CipherData>`
`</EncryptedData>`
`</Order>`
`</SecureCommunicationDemonstration>`

Consider the above xml document from Imran to Ali. Assuming Ali is using sax parser list out pseudo code along with steps used by Ali to locate and decrypt the element back. [5]

Q4. `<?xml version="1.0"?>`
`<!-- An author -->`
`<author>`
`<name gender = "male">`
`<first> Art </first>`
`<last> Gittleman </last>`
`</name>`
`<employeenno>236543</employeenno>`
`</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. [5M]

BITS, Pilani-Dubai Campus
IV th year Second Semester 2008-2009
Degree: B.E.(Hons) Branch: C.S.E

COURSE NO. : CS C 441

**COURSE TITLE : :Selected topics from computer science
(web services and internet based distributed computing
Date : 9-3-2009**

Test1 Time=50 mts Total marks=25 (Closed book) Weightage=25%

Q1.

```
<?xml>
<villain-database>
<villain id="v1">
<name>Darth Vader</name>
<evil>8</evil>
<intelligence>9</intelligence>
<fashion>5</fashion>
</villain>
</villain-database>
```

In the above xml document we want to add an element called `<country>Africa</country>` above the evil element using DOM parser. Outline the steps involved using appropriate pseudo code. [5 M]

Q2..Derive the xml schema for the above XML document given in question1. [5M]

Q3. In a java based component architecture distinguish the difference between stateful session bean and entity bean with appropriate examples. [5M]

Q4. a) what are the important differences between eb-xml and web services ? [3]

b) Specify any two conditions during which document centric web service is preferred compared to RPC oriented web services. [2M]

Q5. Consider a stock quote service hosted in the URL www.stockprice.com and supports a web service by name `stockquote`. The web service, once the name and country of the city is given it will return back the current temperature. outline clearly the messages exchanged during invocation of above web service using http based protocol and Soap based protocol. Make necessary assumptions if required. [5M]

BITS, Pilani-Dubai Campus
IVth Year Second Semester 2008-2009
Degree:B.E.(Hons) Branch:C.S.E

COURSE NO. : CS C 441
**COURSE TITLE : :Selected topics from computer science
(web services and internet based distributed computing
Date : 6-4-2009**

Quiz3

Total marks=5 (Closed book) Weightage=5%

Q1.What is meant by authorization assertion in SAML ?

Q2.What is meant by artifact in browser based SSO profile ?

Q3. Specify any 2 reasons for going for XKMS.

Q4.why there is a need for attribute assertion in SAML ?

Q5.What is the need for validate method of XKISS web service ?

BITS, Pilani-Dubai Campus
IVth Year Second Semester 2008-2009
Degree:B.E.(Hons) Branch:C.S.E

COURSE NO. : CS C 441

COURSE TITLE : :Selected topics from computer science
(web services and internet based distributed computing
Date : 1-4-2009

Quiz2

Total marks=5 (Closed book) Weightage=5%

Q1.what are the advantages of having SSL security compared to application security ?

Q2. How will you retrieve the attributes of an element in a xml document
Using DOM parser?

Q3.Under what circumstances will you prefer DOM over SAX and SAX over DOM?

Q4. suppose you are having a,b,c,d.They are connected to a common network.
They want to do secure conversation using public crypto.
How many keys should be possessed by each node.

Q5. Draw the packet with headers for AH based IP security.

BITS, Pilani-Dubai,Campus

Academic city,Dubai

IV th Year FIRST Semester 2007-08

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

**COURSE NO. : CS UC441 COURSE TITLE: Selected topics from computer science
(web services and internet based distributed computing**

Time :15 mts

Date :25-3-2009

Marks: 5 Quiz1 Closed book

Q1.why there is a need for extending default handler in sax parser ?

Q2.what is meant by play back attack in cryptography?

Q3.justify whether man in the middle attack happen in symmetric crypto ?

Q4. how attributes of an xml document are got using sax parser ?

Q5. Give an example where digital signing is there without confidentiality of information