BITS, Pilani-Dubai Campus,
International academic city
IVth Year Second semester 2011-12

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

CS C441 **Selected topics from computer science**

Compre Exam1 Date:5-6-12 **Total marks=80 (closed book) Weightage=40%**

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

Part-A (5*12=60M)

Q1.a)Outline the techniques you need to adopt during publishing of a web service from a provider in UDDI if the provider and his service need to be quickly discovered by a client. (4M)

b)Suppose I have a weather forecast service which supports the method getweather (String temp)

Suppose I have published the web service under a business with soap over http binding. Now I want to remove the above binding and deliver the web service via soap over SMTP binding. Outline how it can be done ?(4M)

c) What is meant by business key, service key and binding key and when and why they are returned by the UDDI? (4)

Q2.a)what is the main difference between invoking a web application from a browser using synchronous or asynchronous technique?(4M)

b)I want to develop a username and password validation web application where the user using a web form containing text boxes can enter name and password . 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 authenticated user or non authenticated user . That info has to be displayed in the web form. Outline how the above mechanism can be implemented without any hour glass waiting cursor in the browser on clicking the submit button.(8M)

Q3a).In SAML outline the difference between authentication and authorization assertion between a trusted service and a client ?(4M)

b) Outline how using SAML back office transaction a buyer can place order using a seller's web service (that requires proper authentication) assuming that they do not know each other but are known to a trusted service. Specify how the soap request message would look like ?(8M)

Q4.a)Outline any scenario in which cloud computing is the alternative rather than custom hosting of a web application ?(5M)

b)Outline briefly the different types of cloud services that are in the offering and their significance.(4M)

c)Outline three main differences between cloud computing and SOA ?(3M)

Q5.a)Suppose A applies digital signing at application layer level and send the information to B. Suppose an intruder C intercepts the message and replaces the source IP with that of itself. Justify whether B can detect this intrusion n by having integrity at the application layer ? Justify how to detect the above type of intrusion ?(4M)

b)Outline how using SSL security a soap req message can be delivered to a secured web service with confidentiality from a client.(8M)

Part B (4*5=20M)

Q1.Name two important intranet enabled distributed computing protocols, and justify why they can not be used for internet enabled Computing ?(4M)

Q2. Outline how will you find the attributes of the given xml doc using DOM parser ? (4M)

```
<?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>
```

Q3.What are the information you can gather about a web service, using wsdl doc of the same (4M)

Q4.Outloine a scenario in which the contents of the following URL has to be xml digitally signed

http://www.sports.com/homepage.html .

Consider the case where the decrypted signature value of the received xml doc matches with the computed signaturevalue, but the digest in the digestvalue tag do not match with computed digest.

Justify under what circumstances this can happen ?

Q5.Outline briefly how playback attack can be overcome in symmetric and asymmetric cryptography ?[4M]

BITS,Pilani-Dubai campus
Course:Selected Topics from Computer science CS C441
Test2 -Open book Time -50 mts Marks:20
weightage :20% date:16-5-2012

Q1.

```
<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 including http headers(3+3)

Q2. 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 information files using public key cryptography.(2M)

b)At some point of time Alice finds that its private key got corrupted .(2M)

c) or at some point of time Alice finds that its private key got compromised by Trudy. (2M)

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

d)can you comment about the need for following soap request given below?(2)

```
<?xml version="1.0" encoding="utf-8"?>
<LocateRequest xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
Id="I4593b8d4b6bd9ae7262560b5de1016bc"
Service="http://test.xmltrustcenter.org/XKMS"
xmlns="http://www.w3.org/2002/03/xkms#">
<RespondWith>KeyValue</RespondWith>
<QueryKeyBinding>
<ds:KeyInfo>
<ds:X509Data>
<ds:X509Certificate>MIICAjCCAW+gAwIBAgIQlzQov
IEbLLhMa8K5MR/juzAJBgUrDgMCHQUAMBIxEDAOBgNVBAMTB1Rlc3QgQ0EwHhcNMDIwNjEzMjEzMz
Q
xWhcNMzkxMjMxMjM
1OTU5WjAsMSowKAYDVQQGEyFVUyBPPUFsaWNlIENvcnAgQ049QWxpY2UgQWFyZHZhcmswgZ8wDQYJ
K
oZIhvcNAQEBBQADg
Y0AMIGJAoGBAMoy4c9+NoNJvJUnV8pqPByGb4FOJcU0VktbGJpO2imiQx+EJsCt27z/pVUDrexTyc
tC
WbeqR5a40JCQmvN
mRUfg2d81HXyA+iYPl4L6nUlHbkLjrhPPtMDSd5YHjyvnCN454+Hr0paA1MJXKuw8ZMkjGYsr4fSY
pP
ELOH5PDJEBAgMBA
AGjRzBFMEMGA1UdAQQ8MDqAEEVr1g8cxzEkdMX4GAlD6TahFDASMRAwDgYDVQQDEwdUZXN0IENBgh
By
sVHEiNFiiE2lxWv
mJYeSMAkGBSsOAwIdBQADgYEAKp+RKhDMIVIbooSNcoIeV/wVew1bPVkEDOUwmhAdRXUA94uRifiF
fm
p9GoN08Jkurx/gF
18RFB/7oLrVY+cpzRoCipcnAnmh0hGY8FNFmhyKU1tFhVFdFXB5QUglkmkRntNkOmcb8O87xO0Xkt
mv
NzcJDes9PMNxrVt
```

```
ChzjaFAE=</ds:X509Certificate>
                </ds:X509Data>
               </ds:KeyInfo>
          <KeyUsage>Signature</KeyUsage>
              </QueryKeyBinding>
              </LocateRequest>
```

Q3.
```
<?xml version='1.0' encoding='UTF-8'?>
  <SignedPurchaseOrder>
  <PurchaseOrder id="id0" xmlns="urn:purchase-order">
    <Customer>
      <Name>Robert Smith</Name>
      <CustomerId>788335</CustomerId>
    </Customer>
    <Item partNum="C763">
      <ProductId>6883-JF3</ProductId>
      <Quantity>3</Quantity>
      <ShipDate>2002-09-03</ShipDate>
      <Name>ThinkPad X20</Name>
    </Item>
  </PurchaseOrder>
[15] <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
[16]    <SignedInfo>
[17]      <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/
          REC-xml-c14n-20010315"/>
[18]      <SignatureMethod Algorithm="http://www.w3.org/2000/09/
          xmldsig#rsa-sha1"/>
[19]      <Reference URI="#id0">
[20]        <DigestMethod Algorithm="http://www.w3.org/2000/09/
            xmldsig#sha1"/>
[21]        <DigestValue>UfeiscUCL7QkhZtRDLWDPWLpVlA=</DigestValue>
[22]      </Reference>
[23] </SignedInfov
[24] <SignatureValue>
[25]   Ptysg8WdHI2mxwryOOt5I9r9qZm/2gNFNOJyH1Wak4nCUegRpe72tWnsigAKZ
       yopmgUSH3TG
[26]   aGGQF1BTSvk3JUUY/ljrw+5FpTpf3hgZBi7GSWf6WtXqZvMYGUKIlvR/
       421MZg7P9XRUyy37
[27]   ZUzQHtmCYkBorEkEx1J4CYB0G2c=
[28] </SignatureValue>
[29] <KeyInfo>
[30]   <X509Data>
[31]     <X509Certificate>
[32]  MIIDGjCCAoOgAwIBAgICAQAwDQYJKo ... LMAkGA1UEBhMCS1AxETAPBgNVBAgT
[33]  CEthbmFnYXdhMQ8wDQYDVQQHEwZZYW ... TA01CTTEMMAoGA1UECxMDVFJMMRAw
[34]  DgYDVQQDEwdUZXN0IENBMB4XDTAxMT ... xMTAwMTA3MTYxMFowUDELMAkGA1UE
[35]  BhMCS1AxETAPBgNVBAgTCEthbhMQww ... JQk0xDDAKBgNVBAsTA1RSTDESMBAG
[36]  A1UEAxMJU2lnbmF0dXJlMIGfMA0GCS ... NADCBiQKBgQCvnFQiPEJnUZnkmzoc
[37]  MjsseD8ms9HBgasZR0VOAvsbytB18d ... jBdprX+epfF4SLNP5ankfphhr9QXA
[38]  NJdCKpyF3jPoydckle7E7gI9w3Q4NO ... 7OVPqiXIDVlCH4u6GbIoJEpJ57yzx
[39]  dQIDAQABo4HzMIHwMUdEwQCMAAYDVR ... gMCwGCWCGSAGG+EIBDQQfFhlPcGVu
[40]  U1NMIEdlbmVyYXRlZCBDZXJ00ZTAdB ... UYapFv9MvQ9NNnlQ7zgzqka4XORsw
[41]  gYgGA1UdIwSBgDB+gBR7FuT9bLBzIe ... FjpGEwXzELMAkGA1UEBhMCS1AxETA
[42]  BgNVBAgTCEthbmFnYXdhMQ8wDQYDVQ ... AKBgNVBAoTA01CTTEMMAoGA1UECxM
[43]  VFJMMRAwDgYDVQQDEwdUZXN0IENBgg ... BBQUAA4GBALFzGDXMzxJvOnCdJCMZ
[44]  2NsZdz1+wmoYyejB5J6Ch2ygdPeibM ... qr1BNlgSVqA6nyvjHsVIvgBfwx37D
[45]  hJ5hz4azpWu1X22XqyU9fUqoQUtEAd ... JXTFzzvm/3DoEiBkX/BT78YdM8eq0
[46]       </X509Certificate>
```

```
[47]          </X509Data>
[48]        </KeyInfo>
[49]      </Signature>

        </SignedPurchaseOrder>
```

Assume that the above doc is sent to Bob from Alice. Outline how Bob verifies the signature of the above signed document.(3M)

Q4.How the receiver of the below XML part of soap request message will decrypt and understand the contents of soap request message.(3M)

<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>

BITS,Pilani-Dubai campus

CS C441 selected topics from CS

QUIZ-2 Marks:10 Time:20 mts Date:-9-5-2012 weightage:10%

Q1. Outline briefly about Virtual private network ?[2M]

Q2 using simple case study outline how XML encryption compares with simple SSL security?[2 m]

Q3.How will you decrypt the XML doc given below ?[2m]

```
<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>
```

Q4. How a receiver of the given xml doc will validate the signature? [2m]

```
<?xml version="1.0" encoding="UTF-8"?>
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
<SignedInfo Id="foobar">
<CanonicalizationMethod
  Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
<SignatureMethod
  Algorithm="http://www.w3.org/2000/09/xmldsig#dsa-sha1" />
<Reference URI="http://www.abccompany.com/news/2000/03_27_00.htm">
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
<DigestValue>j6lwx3rvEPO0vKtMup4NbeVu8nk=</DigestValue>
</Reference>
<Reference
  URI="http://www.w3.org/TR/2000/WD-xmldsig-core-20000228/signature-
example.xml">
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<DigestValue>UrXLDLBIta6skoV5/A8Q38GEw44=</DigestValue>
</Reference>
</SignedInfo>
<SignatureValue>MC0E~LE=</SignatureValue>
<KeyInfo>
```

```
<X509Data>
<X509SubjectName>CN=Ed Simon,O=XMLSec Inc.,ST=OTTAWA,C=CA</X509SubjectName>
<X509Certificate>
MIID5jCCA0+gA...lVN
</X509Certificate>
</X509Data>
</KeyInfo>

</Signature>
```

Q5.How a receiver of the given doc will verify the integrity of the doc and get the original xml doc ?

. <MyDocument>
<EncryptedData id="encryptedData1">
<EncryptionMethod Algorithm="..." />
<CipherText>
<CipherValue>...</CipherValue>
</CipherText>
<KeyInfo>
<EncryptedKey>
<EncryptionMethod Algorithm="..." />
<CipherText>
<CipherValue>... </CipherValue>
</CipherText>
<KeyInfo>
<X509Data>
<X509Subject>O=HisCompany,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=MyCompany,OU=Engineering,CN=David
Remy</X509Subject>
</X509Data>
</KeyInfo>
</Signature>
</MyDocument>
```

BITS- Pilani,Dubai

IV th Year Second Semester 2012

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

Time :20 mts Date :14-3-2012 Marks: 10 Quiz1 Closed book

Q1. An xml schema is given below:

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema elementFormDefault="qualified"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="Address">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="Recipient" type="xs:string" />
        <xs:element name="House" type="xs:string" />
        <xs:element name="Street" type="xs:string" />
        <xs:element name="Town" type="xs:string" />
     <xs:element name="County" type="xs:string" minOccurs="0" />
      <xs:element name="PostCode">
            <xs:simpleType>
            <xs:restriction base="xs:string">
            <xs:pattern value="[0-9]{5}(-[0-9]{4})?"/>
            </xs:restriction>
            </xs:simpleType>
            </xs:element>
        <xs:element name="Country">
          <xs:simpleType>
            <xs:restriction base="xs:string">
              <xs:enumeration value="FR" />
              <xs:enumeration value="DE" />
              <xs:enumeration value="ES" />
              <xs:enumeration value="UK" />
              <xs:enumeration value="US" />
            </xs:restriction>
          </xs:simpleType>
        </xs:element>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
</xs:schema>
```

Derive an xml doc that conforms to the above schema?[2m]

Q2. What are the events fired by a sax parser for the following XML doc.[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" />
 <flip>
  flip is on
  <dot x="196" y="14" />
  </flip>
</dots>
```

Q3.Using DOM parser I want to parse an XML doc and print the number of child nodes for the root element. Assuming a non validating parser give the snippets of code to achieve the same.[2m]

Q4.

```
POST   /weatherforecast HTTP/1.1
Host: www.weather.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:GetTemp>
                    <m:city>Newyork/m:city>
              </m:GetTemp>
     </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?[2m]

Q5.Consider a credit card validator application which requires the name of the holder and value of the Credit card number. I want to implement the same using RPC web service and simple web enabled application. How the invocation of the credit card validator differs in both the cases ?[2m]