BITS, Pilani-Dubai Campus

IV th year First Semester 2011-2012

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

COURSE TITLE : :Selected topics from computer science

COURSE NO. : CS C 441

Date : 12-1-2012

Compre exam Total marks=80

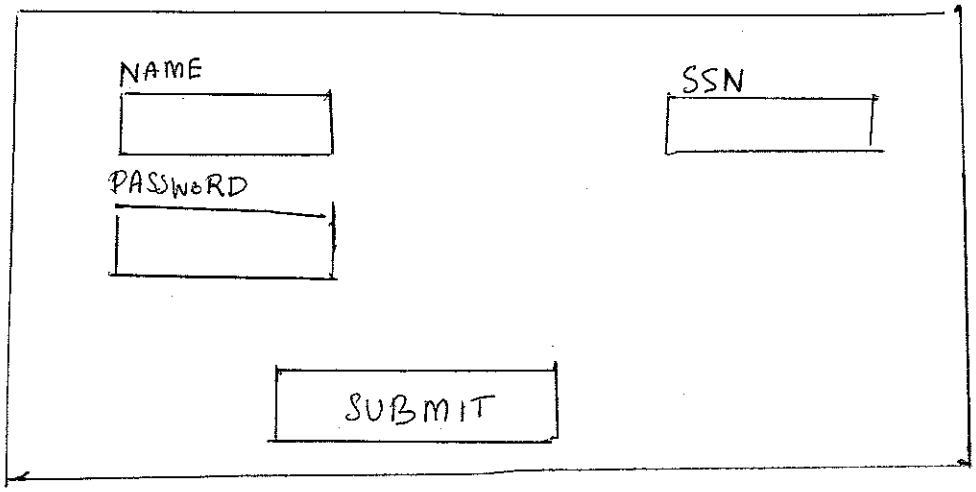
(closed book Weightage=40%)

Part-A(Answer all the questions: 5*10=50M)

Q1. Suppose A and B want secured communication using asymmetric cryptography. Let the application running in A or B need not have the overhead of certificate processing logic. Each one of them can generate their own private key and public key. Let A wishes to use a X.509 certificate and B wish to use a PGP certificate. If any of them lost their private key appropriate protection measures need to be taken .Both A and B do not want direct communication with certificate provider to avoid software overhead. Outline a mechanism using which the above things can be achieved with applications A and B (10)

Q2.a) outline the significance of browsing experience faced by user when handling ajax enabled web form submission and validation with that of non-ajax enabled one.(4M)

b) Given the block diagram of a web form application. Here the user should enter his name and password and based on that his social security number will be displayed in another text box after he submits the web form. The submission of the web form should invoke a searchnumber.php running on a server whose url is www.urlfinder.com and without any hour glass waiting the result should appear in the text box.Outline how this can be done?(6M)



Q3.a)what are the advantages of going for cloud computing compared to conventional web computing? (4M)

b)Enumerate the types of services offered by the cloud ? (4M)

c) compare the the SOA with that of cloud computing.(2 M)

Q4.a) Suppose A wants to access an online air ticket booking web portal by logging into the portal to book tickets for Sydney. Similarly he needs to book hotel using another web portal and rent a car using one more portal. Outline a mechanism how the above things can be carried out with single sign on assuming that A uses single sign on using browser profile of SAML?(10M)

Q5. a)

```
<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>
```

Can you comment upon the nature of the above soap req message ?List out the steps involved about the handling of the above message by the receiver ?(6M)

b)

```
<?xml version='1.0'?>
<PaymentInfo xmlns='http://example.org/paymentv2'>
 <Name>John Smith<Name/>
 <CreditCard Limit='5,000' Currency='USD'>
  <Number>4019 2445 0277 5567</Number>
  <Issuer>Bank of the Internet</Issuer>
  <Expiration>04/02</Expiration>
 </CreditCard>
</PaymentInfo>
```

Assume that A wants to send the credit card element in the XML in confidential manner to B. Let A and B have exchanged the necessary keys for securing well in advance. Outline how the resultant xml doc from A(meant for B)would look like ?(4M)

Part-B(answer all the questions 5*6=30M)

Q1.Consider the snippets of the code given below:

```
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");
     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();
}
```

a) What will be the contents of output.xml file ?(4)
b) Suppose I want to append an element within Book as a last element as shown below.
   <Publishyear country="India"> 2011</Publishyear>
   Specify the java code to do that (2M)

Q2. Briefly outline the steps involved in publishing a web service by a business in UDDI ?(6M)

Q3.waht are the events fired by SAX parser when it parses the XML doc given below.(4M)

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

Briefly outline how the attribute of the element name can be obtained using sax parser?(2M)

Q4.How a client of the web service will do authentication using binary token ?(6M)

Q5. perform enveloped xml signature of the purchase order element(6 M)

```
<?xml version="1.0" encoding="UTF-8"?>
<PurchaseOrder id="25">
<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>
</PurchaseOrder>
```

BITS, Pilani-Dubai Campus

IV th year First Semester 2011-2012

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

COURSE TITLE : :Selected topics from computer science

COURSE NO. : CS C 441

Date : 22-12-2011

Test2 Total marks=20 (open book) Weightage=20% open book

Q1. Perform XML digital signing for the Transaction element and encryption of the CreditCard element in the same output. Assume that the sender and receiver have not exchanged any certificates before the above process.[5m]

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<PaymentInfo>
  <Name>John Doe</Name>
    <Transaction Id="25">
<CreditCard Limit='5,000' Currency='USD' Id="30">
   <Number>1234 5678 90123 4567</Number>
   <Issuer>My Bank</Issuer>
   <Expiration>04/06</Expiration>
  </CreditCard>

 </Transaction>
</PaymentInfo>
```

Q2.What is meant by VPN and with the help of a diagram outline how it can be implemented?[5M]

Q3.when a client invokes a web service that requires authentication, how a password enabled digest from the soap client will lead to[2.5 +2.5}

a) prevention of playback attack during authentication

b) proper authentication of the client

Q4.What is IP spoofing ? 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 by having security at the application layer? Justify how to detect the above type of intrusion.[2 +3]

BITS, Pilani-Dubai Campus

IV th year First Semester 2011-2012

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

COURSE NO. : CS C 441 **COURSE TITLE : :Selected topics from computer science**

Date : 3-11-2011

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

Answer all the questions

Q1.Given the wsdl doc shown below .Derive the soap req and soap resp for the web service.?[5M]

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

   <message name="GetStockRequest">
      <part name="Stocksymbol" type="xsd:string"/>
   </message>
   <message name="GetStockResponse">
      <part name="price" type="xsd:string"/>
   </message>

   <portType name="Stockquote_PortType">
      <operation name="GetStock">
```

```
        <input message="tns:GetStockRequest"/>
        <output message="tns:GetStockResponse"/>
    </operation>
</portType>

<binding name="Stockquote_Binding" type="tns:Stockquote_PortType">
    <soap:binding style="rpc"
        transport="http://schemas.xmlsoap.org/soap/http"/>
    <operation name="GetStock">
        <soap:operation soapAction="GetStock"/>
        <input>
            <soap:body
                encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
                namespace="urn:examples:Stockquoteservice"
                use="encoded"/>
        </input>
        <output>
            <soap:body
                encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
                namespace="urn:examples:Stockquoteservice"
                use="encoded"/>
        </output>
    </operation>
</binding>

<service name="Stockquote_Service">
    <documentation>WSDL File for StockquoteService</documentation>
    <port binding="tns:Stockquote_Binding" name="Stockquote_Port">
```

```
        <soap:address
            location="http://www.stockquote.com/soap/servlet/stockquote"/>
      </port>
   </service>
</definitions>
```

Q2.An XML document is given below. I want to insert an element <fulltime>yes</fulltime>,

in the xml tree of the XML doc, above the element by name EmpID.

Using java code or pseudo code outline the steps involved step by step.[5M]

```
<?xml version="1.0"?>
<ORGANISATION>
<NAME> Admin </NAME>
<member>Arun </member>
<EmpID>2010</NAME>
</ORGANISATION>
```

Q3. Using sax parser I want to parse the xml doc given below. I want to print the text within an element only if the element has some attribute. Outline the steps involved in the same using java code or pseudo code. [5M]

```
<?xml version="1.0"?>
<!-- Books written by an author -->
<author>
<book>
 <title full="true">Computing with Java</title>
  </book>
   <book >
   <title>Objects to Components with the Java Platform</title>
   </book>
  </author>
```

Q4. Microsoft wants to host an online catalogue web service using which customers can know the prices of various products offered by the company. Microsoft wants to ensure that customers should be able to locate the business and service quickly when searching via uddi. Outline the steps used by Microsoft to publish the web service in uddi?[5M]

BITS, Pilani-Dubai

IVth Year First semester 2011-12

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

Selected topics from computer science PART-A

COURSE NO. : CS C441

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

Quiz2 Date:12-12-11

1. *Justify whether man in the middle attack can happen in symmetric key cryptography.[2m]*

2. *In public key cryptography if the private key of mine gets compromised what I have to do immediately ? why ? (2M)*

3. *What does it mean for a signed document to be verifiable, non-forgible, and non-repudiable?[2M]*

4. KeyPairGenerator keyGen = KeyPairGenerator.getInstance("RSA");

```
keyGen.initialize(1024);
KeyPair key = keyGen.generateKeyPair();
Cipher cipher = Cipher.getInstance("RSA/ECB/PKCS1Padding");
System.out.println( "\nStart encryption" );
cipher.init(Cipher.ENCRYPT_MODE, key.getPrivate());
byte[] cipherText = cipher.doFinal(md);
```

I want to decrypt the information encrypted by the above code. Provide the lines of code to achieve the same.[1]

5. ✓

```
KeyGenerator keygen = KeyGenerator.getInstance("DES");
SecretKey key = keygen.generateKey();
Cipher cipher = Cipher.getInstance("DES/ECB/PKCS5Padding");
cipher.init(Cipher.ENCRYPT_MODE, key);


File f = new File("C:\\Users\\Vadivel\\Documents\\input.txt");
FileInputStream in = new FileInputStream(f);
plainData = new byte[(int)f.length()];
```

```
                in.read(plainData);

                encryptedData = cipher.doFinal(plainData);

                FileOutputStream target = new FileOutputStream(new
File("C:\\Users\\Vadivel\\Documents\\modified.txt"));

                target.write(encryptedData);

                target.close();
```

List out (only) the important steps carried out by snippets of code given above ?[2m]

6.Distingusih between Certificate authority and KDC[1]