มหาวิทยาลัยสงขลานครินทร์

คณะวิศวกรรมศาสตร์ ภาควิชาวิศวกรรมคอมพิวเตอร์

การสอบไล่ปลายกลางภาคการศึกษาที่ 2 **ประจำปีการศึกษา 2548**

วันที่พฤหัสบดีที่ 2มีนาคม 2549 **เวลา 0900-1200 น**

วิชา 240-526 Computer and Information Security **ห้องสอบ R300**

ไม่อนุญาตให้นำเอกสารเข้าในห้องสอบ

ทำข้อสอบทุกข้อ

เขียนคำตอบในกระดาษข้อสอบนี้

คะแนนเต็ม 100 คะแนน

ทุจริตในการสอบ โทษขั้นต่ำคือ

ปรับตกในรายวิชาที่ทุจริต และพักการเรียน 1 ภาคการศึกษา

ข้อ 1 จงอธิบายการทำงานของระบบ Security ที่ท่านได้รับการมอบหมายให้ออกแบบใน Assignment 1 ในห้องเรียน โดยนำเสนอในรูปแบบของ คำอธิบายประกอบ Diagrams (10 คะแนน)

ข้อ 2

จาก XML listing ที่ให้ จงอธิบายการทำงานของ SOAP header ที่ใช้ Digital Signature (DS) ว่าแต่ และ element และ child element ของมันทำหน้าที่อะไร อย่างไร บ้าง (10 คะแนน)

```
<SOAP-ENV:Header>
    <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="#GetSpecialDiscountedBookingForPartners">
                <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>
                    BIUddkjKKo2...
                </ds:DigestValue>
            </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>
        </ds:SignatureValue>
        <ds:KeyInfo>
        </ds:KeyInfo>
    </ds:Signature>
</SOAP-ENV:Header>
```

ข้อ 3

3.1 XML firewall ดำเนินการ XML Encryption Processing อย่างไรบ้าง (4 คะแนน)

3.2. จาก XML listing ของ SOAP message ที่กำหนด จงอธิบายการใช้ Web Services Security (WSS) specification จาก OASIS เพื่อกำหนด mechanism เพื่อแลกเปลี่ยน SOAP messages ในแง่ของ Message Integrity ,User Authentication และ Confidentiality (6 คะแนน)

```
<?xml version="1.0" encoding="utf-8"?>
<SOAP:Envelope
   xmlns:SOAP="http://www.w3.org/2001/12/soap-envelope"
    xmlns:wsse="http://schemas.xmlsoap.org/ws/2002/xx/secext"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
   <SOAP:Header>
       <wsse:Security>
       <wsse:BinarySecurityToken
          ValueType="wsse:X509v3"
         EncodingType="wsse:Base64Binary"
          wsu:Id="MyTourOperatorCertificate">
          LKSAJDFLKASJDlkjlkj243kj;lkjLKJ...
       </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="#myDiscountRequestBody">
          <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>BSDFHJYK21f...</ds:DigestValue>
        </ds:Reference>
      </ds:SignedInfo>
      <ds:SignatureValue>
        GKLKAJFLASKJ52kjKJKLJ345KKKJ...
      </ds:SignatureValue>
       <ds:KeyInfo>
          <wsse:SecurityTokenReference>
          <wsse:Reference URI="#MyTourOperatorCertificate"/>
       </wsse:SecurityTokenReference>
     </ds:KeyInfo>
     </ds:Signature>
  </wsse:Security>
</SOAP:Header>
<SOAP-ENV:Body>
  <s:GetSpecialDiscountedBookingForPartners
    xmlns:s="http://www.MyHotel.com/partnerservice/"
     ID="myDiscountRequestBody">
        <!--Parameters passed with the method call-->
    </s:GetSpecialDiscountedBookingForPartners>
```

```
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

ข้อ 4

4.1 Security Markup Language(SAML) คืออะไร ทำหน้าที่อะไรในระบบ security ยกตัวอย่างการประยุกต์ใช้งาน(4 คะแนน)

4.2 จาก XML listing ที่ให้มา จงอธิบายการทำงาน ของ SAML assertion โดยมีโจทย์ประกอบคือ The tour operator application requests an assertion from the marketplace (a SAML authority). The tour operator is a requester application and the subject of the assertion as well. After getting the assertion from the marketplace, the tour operator wraps the assertion in a WSS message and send the WSS message to the hotel application. The hotel relies on the assertion to decide whether to allow the tour operator the special discount or not. (6 คะแนน)

```
<?xml version="1.0" encoding="utf-8"?>
<Assertion
    xmlns="urn:oasis:names:tc:SAML:1.0:assertion"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
```

```
    MajorVersion="1"
    MinorVersion="0"

AssertionID="http://www.myEMarketPlace.com/AuthenticationService/SAMLAssertions/786"
    Issuer="http://www.myEMarketPlace.com"
    IssueInstant="2003-03-11T02:00:00.173Z">
    <Conditions
      NotBefore="2003-03-11T02:00:00.173Z"
      NotOnOrAfter="2003-03-12T02:00:00.173Z"/>
    <AuthenticationStatement
      AuthenticationMethod="urn:ietf:rfc:3075"
      AuthenticationInstant="2003-03-11T02:00:00.173Z">
      <Subject>
          <NameIdentifier
          NameQualifier="http://www.myEMarketPlace.com">
          MyTourOperator
        </NameIdentifier>
        <SubjectConfirmation>
            <ConfirmationMethod>
            urn:oasis:names:tc:SAML:1.0:cm:holder-of-key
          </ConfirmationMethod>
          <ds:KeyInfo>
            <ds:KeyName>MyTourOperatorKey</ds:KeyName>
            <ds:KeyValue> ... </ds:KeyValue>
          </ds:KeyInfo>
        </SubjectConfirmation>
      </Subject>
    </AuthenticationStatement>
   <ds:Signature>...</ds:Signature>
</Assertion>
```

ข้อ 5 จงอธิบายการทำงานของระบบ Security ของระบบ Third Generation Cellular Mobile Telecommunication System (3G) และเน้นที่ข้อดีของระบบที่ได้ปรับปรุงให้ดีกว่าระบบ GSM ที่นักเรียนแต่ละคนได้รับการมอบหมายให้ออกแบบใน Assignment โดยนำเสนอในรูปแบบของคำอธิบายประกอบ Diagrams (10 คะแนน)

ข้อ 6 จงอธิบายการทำงานของระบบ Security ของ Overall Mahosot Global Systems Services(MGSS) ที่นักเรียนแต่ละคนได้รับการมอบหมายให้ออกแบบใน Assignment โดยนำเสนอในรูปแบบของ คำอธิบายประกอบ Diagrams(10 คะแนน)

ข้อ 7 จงอธิบายการทำงานของระบบ Security ของ JAVA Security ที่นักเรียนแต่ละคนได้รับการมอบหมายให้ออกแบบใน Assignment โดยนำเสนอในรูปแบบของ คำอธิบายประกอบ Diagrams (10 คะแนน)

ข้อ 8

จงอธิบายการทำงานของระบบ Security ของ Security in Mahosot Global Systems Services(MGSS) Nervous Subsystem โดยเน้นเครือข่ายแบบที่เป็น WSireless คือ 2G/3G, WiFi และ WiMaxที่นักเรียนแต่ละคนได้รับการมอบหมายให้ออกแบบใน Assignment ซึ่งเริ่มต้นจากการอธิบาย Systems Architecture สำหรับ MGSS โดยนำเสนอในรูปแบบของ คำอธิบายประกอบ Diagrams (15 คะแนน)

ข้อ 9.1

จงอธิบายการทำงานของระบบ Security ของ Federated Identity เพื่อประยุกต์ในการใช้งาน Security แบบ Single Sign On (SSO) ตาม concept เบื้องต้นของ Liberty Allianceที่นักเรียนแต่ละคนได้รับการมอบหมายให้ออกแบบใน Assignment โดยนำเสนอในรูปแบบของ คำอธิบายประกอบ Diagrams (7 คะแนน)

ข้อ 9.2

จงอธิบายการทำงานของระบบ Security ของ RSA Technology Security ที่นักเรียนแต่ละคนได้รับการมอบหมายให้ออกแบบใน Assignment โดยเน้นที่การประยุกต์ใช้งานของแต่ละ algorithm ที่สำคัญที่ยกตัวอย่างมา (8 คะแนน)