Corso di Sicurezza delle Architetture Orientate ai Servizi
Prof. E. Damiani
14-2-2011

Potete tenere libri e appunti. NON scrivete su questo foglio.
Scrivete IN STAMPATELLO nome, cognome e numero di matricola su tutti i fogli che consegnate.

Esercizio 1 (9 punti) Considerate il seguente messaggio SOAP:

```
<soap:Envelope>
  <soap:Header>
    <wsa:To>http://stock.contoso.com/realquote</wsa:To>
    <wsa:Action>http://stock.contoso.com/GetRealQuote</wsa:Action>
  </soap:Header>
  <soap:Body>  BODY OMITTED </soap:Body>
</soap:Envelope>
```

a) (3 punti) Spiegate il significato di tutti i marcatori e dei prefissi di namespace utilizzati.
b) (3 punti) Elencate i marcatori aggiuntivi che sarebbero necessari per firmare il messaggio
c) (3 punti) Discutete il loro significato

Esercizio 2 (21 punti) Considerate il seguente header di un messaggio SOAP crittato:

```
<?xml version="1.0" encoding="UTF8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
<SOAP-ENV:Header>
 <wsse:Security xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
     xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
     xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
     xmlns:xenc="http://www.w3.org/2001/04/xmlenc#" SOAP-ENV:mustUnderstand="1">
  <wsse:BinarySecurityToken EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
soap-message-security-1.0#Base64Binary" 1 ValueType=http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-x509-token-profile-1.0#X509 wsu:Id="x509cert00">
  </wsse:BinarySecurityToken>
  <xenc:EncryptedKey xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
   <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/> 2
   <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <wsse:SecurityTokenReference>
     <wsse:Reference URI="#x509cert00" ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-x509-token-profile-1.0#X509"/>  3
    </wsse:SecurityTokenReference>
   </ds:KeyInfo>
   <xenc:CipherData>
   <xenc:CipherValue>M6bDQtJrvX0pEjAEIcf6bq6MP3ySmB4TQOa/B5UlQj1vWjD56V+GRJbF7ZCES5ojwCJHRVKW1ZB5 4
                     Mb+aUzSWlsoHzHQixc1JchgwCiyIn+E2TbG3R9m0zHD3XQsKTyVaOTlR7VPoMBd1ZLNDIomxjZn2
                     p7JfxywXkObcSLhdZnc=</xenc:CipherValue>
   </xenc:CipherData>
   <xenc:ReferenceList>
    <xenc:DataReference URI="#Enc1"/>
   </xenc:ReferenceList>
  </xenc:EncryptedKey>
 </wsse:Security>
</SOAP-ENV:Header>
<SOAP-ENV:Body>
                              BODY OMITTED
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Discutete le seguenti affermazioni, **spiegando se sono vere o false**

a. (3 punti) Il messaggio è protetto tramite un sistema di crittografia simmetrica, la cui chiave è crittata con la chiave pubblica del destinatario
b. (5 punti) Il security token contiene la codifica base64binary del certificato X.509, compresa la chiave pubblica usata per crittare la chiave simmetrica
c. (3 punti) Non è possibile dedurre da questo header l'algoritmo usato per crittare la chiave simmetrica
d. (4 punti) Lo header contiene un riferimento all'algoritmo usato per crittare il messaggio