Opgave 1

1. Leg de algemene filosofie achter REST uit aan de hand van internetbronnen. Gebruik in je uitleg de term resource en beschrijf ook hoe een URL er uit kan zien bij het aanroepen van een resource.

REST is een architectuur stijl voor het ontwerpen van web services. REST maakt gebruik van de bestaande architectuur van het World Wide Web. In REST staan resources centraal. Resources zijn objecten die gedeeld kunnen worden tussen computers, dit kunnen afbeeldingen, muziek, tekst of bestanden zijn. Resources worden aangeroepen met behulp van URI’s, op deze URI’s worden “http verbs” (werkwoorden) uitgevoerd zoals GET, POST, PUT en DELETE. Hiermee wordt de bestaande architectuur van het internet (WWW) gebruikt om te communiceren tussen resource providers.  
Het opvragen van een boek zou bijvoorbeeld met een GET request op de volgende URL gebeuren: <http://book-store.com/api/books/113> waarbij 113 het id van het desbetreffende boek is.

(bron <http://www.xml.com/pub/a/2004/12/01/restful-web.html>)

1. Rest maakt gebruik van het http protocol op manieren die het meer performance en minder overhead geven (http caching, proxy). In REST is er geen WSDL aanwezig die overhead inneemt. De mogelijkheden van de REST service is op te vragen met een http OPTIONS. SOAP werkt alleen in XML, REST kan in meerdere formaten gebruikt worden die minder overhead hebben.

Opgave 3

a)   
  
Vertrouwelijkheid is een vorm van privacy. Niet alle gegevens mogen toegankelijk zijn aan iedereen. Bijvoorbeeld een BSN van een persoon is een vertrouwelijk gegeven, die misbruikt kan worden wanneer derden hem achterhalen

Authenticatie houdt in dat een partij zich moet melden bij een beheerder om zichzelf bekend te maken. Op deze manier weet de beheerder wie de partij is en wat zijn rechten zijn. Je wilt bij een webservice weten wat voor rechten gebruikers hebben, daarom moet je ze laten authentiseren om het te gebruiken.

Integriteit is het beschermen van informatie/data gedurende het beheer ervan zodat deze valide blijft. Ongeoorloofde partijen mogen de informatie niet aanpassen. Wanneer derden je informatie kunnen aanpassen door bijvoorbeeld lukraak PUT’s uit te voeren, is je data niet meer juist.

Onweerlegbaarheid houdt in dat het verzenden en ontvangen van informatie niet ontkend kan worden door de betrokken partijen. Er is controle op de transactie tussen de betrokken partijen, die te zien valt door de betrokken partijen en eventueel derden. Dit is belangrijk zodat je weet wie welke data heeft opgevraagd in je webservice.

B) Een digitale handtekening is een handtekening die de verstuurder van een bericht digitaal plaatst in het bericht om zijn authenticiteit te geven.

Hashing is het versleutelen van een bericht met een (willekeurige) waarde, zodat het bericht niet meer leesbaar is. Het versleutelde bericht wordt dan verstuurd naar de ontvanger die het vervolgens kan decoderen en lezen.

Symmetrische encryptie is een vorm van versleuteling waarin de sleutel voor het coderen en decoderen van het bericht hetzelfde is en dus geheim moet blijven voor de verstuurder en ontvanger.

In asymmetrische encryptie verschilt de sleutel voor het coderen van een bericht van de sleutel voor het decoderen. Er is een publieke sleutel en een private sleutel. De publieke sleutel kan gebruikt worden om te laten zien dat het bericht van de verstuurder afkomstig is en derden kunnen specifieke berichten versleutelen voor de eigenaar van deze publieke sleutel. De geheime sleutel wordt door de ontvanger gebruikt om berichten die bedoelt zijn voor hem te decoderen, en om berichten te encoderen die hij verstuurd naar anderen.

C) Digitale Handtekening – Authenticatie  
Hashing – Vertrouwelijkheid, Integriteit  
Symmetrische encryptie – Integriteit, Authenticatie  
Asymmetrische encryptie – Integriteit, Authenticatie

D) Omdat asymmetrische encryptie een stuk complexer is en dus meer resources/tijd kost, daarnaast schaalt de overhead van de encrptie lineair mee en maakt het dus bij grotere bestanden erg groot.

E) ECB is Eletronic Codebook, de simpelste encryptie modus. Het bericht wordt in blokken opgedeeld en vervolgens per blok gecodeerd.  
De methode die wordt gebruikt is de Propagating Cipher Block Chaining.

F) Eerst wordt het bericht in stukken opgedeeld, de karakters een voor een in een int array gezet. Vervolgens wordt er een SHA-0 hashing algoritme toegepast waarin blokken van 512 bits worden aangemaakt en de versleuteling 80 rondes lang gebeurt.

Opgave 6

1. Het verschil tussen queue en topic is dat een bericht in een queue naar één subscriber/ontvanger gaat. Een topic gaat naar alle subscribers/ontvangers.
2. Een ESB verschaft een abstracte laag over messaging middleware. Daarnaast biedt het met een eventbus mogelijkheden voor complexere architectuur en kan het berichten transformeren en routen naast het bijhouden (monitoren) van het berichtensysteem.  
   Daarbij kunnen functies als logging, beveiliging en administratie worden gebruikt.
3. Ja, met een ESB had de messaging ook geïmplementeerd kunnen worden. In plaats van JMS queues en topics kan er met de eventbus in ESB gewerkt worden om de berichten te routeren naar de specifieke nodes. De implementatie daarvan ligt aan de specifieke ESB.
4. BPEL is een web service standaard gebaseerd op XML. Je gebruikt ESB wanneer je 2 of meer systemen wilt verbinden, BPEL is een software implementatie. BPEL wordt gebruikt voor lange processen die stateful zijn.