



W1-2-60-1-6

**JOMO KENYATTA UNIVERSITY OF AGRICULTURE AND TECHNOLOGY
UNIVERSITY EXAMINATIONS 2017/2018**

EXAMINATIONS FOR THE DEGREE OF MASTER OF SCIENCE IN COMPUTER ENGINEERING.

ICS 3114 WEB TECHNOLOGY

DATE: FEBRUARY 2018

TIME: 3 HOURS

Instructions:

Answer Question ONE and any other TWO Questions from this paper.

QUESTION ONE.

- a) Define the term socket and briefly differentiate between the two essential types of sockets. (4marks)
- a) Define ontology as used in semantic web, clearly showing its elements and with the aid of an example, show the steps followed in building ontology for a given domain. (6marks)
- b) Today there are no projects or applications that don't have a REST API for the creation of professional services based on this software. Twitter, YouTube, Facebook identification systems. Hundreds of companies generate business thanks to REST and REST APIs. Without them any horizontal growth would be practically impossible.

Required:

- i) Discuss with the aid of illustrations what is meant is implied by this statement. (6marks)
- ii) Describe architectural principles of REST in detail. (6marks)
- c) Cryptographic signatures provide extremely strong proof that a message has not been altered and was signed by a specific key. (6marks)

Describe some alternative mechanisms that provide some assurance of the origin and verification of the message's integrity. (4marks)

d) Given the sentence:

The students of the course s:Digital Design are „Peter“, „Paul“ and „Mary“.

And also given that the resource for the RDF statement in (d) is

"http://www.w3schools.com/rdf":

Required:

Give a simplified RDF document to describe the given resource.

(4marks)

QUESTION TWO.

a) With the aid of a well-labeled diagram, illustrate a standard model that can be used for securing information flow over an insecure communications channel, in the presence of possible opponents.

(6marks)

b) Given a plaintext message P , given the public key pair (e, n) and that the private key consists of (d, n) . One application of the public-key cryptography is the one suggested by Diffie and Hellman, known as the digital signature.

Explain why we say this concept is similar in properties to handwritten signatures.

(2marks)

c) Given that for the RSA cryptosystem, the original input message (the plaintext m), and the output c as the resulting ciphertext, then the public key for the cryptosystem consists of the modulus value n , the public exponent value e , which is the $\gcd(e, \phi(n))=1$; as a value $e=7$ (and the private exponent is d). A pair of random primes p and q , are generated, whose values are: $p=5$ and $q=11$.

b) i) Compute product n

(2mark)

ii) Compute the modulus, $\phi(n)$

(2mark)

Given that we choose e , the gcd, as a value $e=7$, determine

i) Publish public key K_U .

(2mark)

ii) The secret private key K_R .

(2mark)

d) Using the given gcd and given that a plaintext message $m = 2$, calculate the encryption, and show that the computation it gives a result of the original plaintext.

(4marks)

QUESTION THREE.

- a) When the World Wide Web went live in 1991, it consisted of static pages of text connected to each other by hyperlinks, and that's pretty much what it remained for years. But from the outset, the Web's inventor, Tim Berners-Lee, had envisioned a much more sophisticated Web, a so-called Semantic Web, which wouldn't just store data but would actually know what it meant. In fact, an existing Semantic Web standard, the Web Ontology Language, solves this problem.
- i). Explain the semantic web concept as discussed in the given case. (4marks)
- ii). Describe how ontology as used in semantic web standard can be used to store data and get the meaning out of the same data. (6marks)
- b) Describe the major difference between the RDF and XML. (4marks)
- c) Given that the company is identified by the following URI
<http://www.w3.org/Organization/contact#WebifySolutions>; and
that its name is Webify Solutions, its e-mail address is info@webifysolutions.com, and its phone number is 1-800-4WEBIFY.

Required:

Express the given information as an RDF listing that makes a statement about the company resource.

(6marks)

QUESTION FOUR.

- a) Just because our name is SoapUI, doesn't mean that we also don't know what we are talking about when it comes to explaining RESTful web services and APIs. As one REST API tutorial put it: SOAP is like an envelope while REST is just a postcard.

Required:

Describe what is meant by this statement.

(4marks)

- b) Name and explain the *differences between SOAP and REST APIs, clearly indicating the conditions under which each can be chosen for a web project.*

(6marks)

- c) SOAP relies heavily on XML, and together with schemas, defines a very strongly typed messaging framework.

- i) Discuss what is meant by this statement

(6marks)

- ii) Describe SOAP and briefly state how it relates to XML.

(4marks)

QUESTION FIVE.

a) Microsoft's Active Server Pages (ASP) technology is a powerful tool for building Web sites that incorporate dynamic content, like pages built from databases. Initially released as an add-on to Internet Information Services (IIS) via the Windows NT 4.0 Option Pack it is included as a free component of Windows Server (since the initial release of Windows 2000 Server). The ASP application-development framework includes a number of objects.

b) Describe how ASP is used for building a dynamic website.

(4marks)

c) Name three objects used by ASP and with the aid of an example, show they can be used in web development.

(6mark)

b) Create an Asp page using VBScript, called showdays.asp, whose sole responsibility is to generate days of the week.

(6marks)

c) Define the term socket and briefly differentiate between the two essential types of sockets.

(4marks)

b)

c)