EASTERN UNIVERSUTY, SRI LANKA

DEPARTMENT OF MATHEMATICS
SPECIAL DEGREE EXAMINATION IN COMPUTER SCIENCE - 2008/2009
PART - I

CS 407 - INTERNET SECURITY

Calculators are allowed

Answer All Questions Time Allowed: Two Hours

1.

(a) Suppose we have nodes A, B, C and D in a network. How many keys do we have to generate such that A, B can communicate with C and D in a bidirectional secure way using the AES encryption algorithm.

(5 marks)

(b) We now replace AES in (a) above with a public key system. How many public keys do we have to generate in this case such that A, B can communicate with C and D in a bi-directional secure way.

(5 marks)

(c) Suppose that we have 100 nodes in a network. How many AES keys do we need such that every pair of nodes can communicate in a safe way?

(5 marks)

(d) Suppose that we have 100 nodes in a network. How many public keys do we need such that every pair of nodes can communicate in a safe way?

(5 marks)

(e) A 128 bit AES key is required to be broken using the brute force method on a 1GHz computer. How long would it take to break the key in the best case and in the worst case situations? Assume that 1000 clock cycles are required to check a single AES key.

(5 marks)

2.

(a) What is the main difference between HASH and HMAC?

(5 marks)

(b) List five characteristics of a good cipher.

(5 marks)

(c) What is the greatest common divisor of 1970 and 1066?

(5 marks)

(d) Suppose we want to use the RSA scheme for an encryption and have chosen the integer 77 as the product of 2 prime numbers p and q. For the private key d and public key e, we have the relation $e*d = 1$ *modulo* $(p-1)$ $(q-1)$.

(i) What is the private key d for a public key $e = 7$?

(ii) What is the cipher C for a message M =26?

(10 marks)

3.

(a) What is the purpose of a “Digital Certificate"?

(8 marks)

(b) Using a block diagram, briefly explain the operation of the .NET passport protocol.

(9 marks)

(b) Compare and contrast SET and 3-D secure protocols

(8 Marks)

4.

(a) Amal would like to use the hybrid symmetric/asymmetric key crypto system to send a signed and encrypted message to Kamala. What are the necessary steps to be followed in:

- the creation process and
- the verification process.

(8 Marks)

(b) Write a simple Java program to create a hash of a file called “hello.txt” using Java Cryptography Extension (JCE).

(9 Marks)

(c) How do you create a signed Java applet?

(8 Marks)

****