Kathmandu University

Information Security and Cryptography
COMP(560) [1]

SUPPLEMENTARY EXAM

Duration : 120 minutes
Answer all questions
All questions carry equal marks
Your answers should be brief, precise, and to the point.
Write legibly. You may lose marks if your answers are not legible.

Ref.: q201112.tex
Date: 2011/12/??

1. In PKI systems what is a root certificate ?

2. In the GPG model of trust, what exactly is trust ?

3. Is the GPG model of trust an equivalence relation ? What subrelations of equivalence does it obey ?

4. What is a certificate revocation list in PKI systems ?

5. What aspect of a key determines its security against brute force attacks ? Why ?

6. Can web cookies be a threat to security ? What risks, if any, do they cause ?

7. Is DDOS a passive attack or an active attack ?

8. Why is IPV6 considered more secure than IPV4 ? Give two reasons.

9. Prove :

   If m is a positive integer, and $a \equiv b\ mod(m)$ and $c \equiv d\ mod(m)$ then $a\ +\ c\ \equiv b\ +\ d\ mod(m)$

[1] Prepared by : Dr. Partha (drpartha@gmail.com)
This document, and the suggested solutions will be published on the w-w-web after 15 Dec. 2011. Details will be announced in Prof. Partha's blog

10. What is *malicious logic* ?

11. Why is it a good idea to compress a message before encrypting it ?

12. What is meant by *rotating log files* ? Why is it necessary ?

13. How is port scan useful in enforcing security ?

14. Which of the following are used in vulnerability analysis :

    - Carmen's test
    - penetration testing
    - port scan
    - modulo arithmetic
    - digital signature

    Give a short (two line description) for the choice you make.

15. Why is SSL/TLS not used for securing client-client communication ?

16. What is *the avalanche effect* in hash digests ? How is it useful ?

17. Why is the logical XOR operator popular for encryption (and decryption) ? Give an example of usage of XOR cipher.

18. Why is it a more secure option to let web browsers accept only session cookies (valid only for the current session), rather than persistent cookies ?

19. What is a hash salt ? How is it commonly used ?

20. Why does GPG use the private key for creating a digital signature ?

* * *