Kathmandu University

Information Security and Cryptography
COMP(560) [1]

Duration : 120 minutes
Answer all questions
All questions carry equal marks
Your answers should be brief, precise, and to the point.

Ref.: CS560-2011
Date: 2011/11/30

1. Explain at least one situation where one-way encryption is useful.
2. Give the first 15 elements of the Fibonacci series in
   - mod 3 arithmetic
   - mod 5 arithmetic

   What pattern do you notice ? Why ?
3. When issuing a digital certificate, why does the Certifying Authority insist on your presence in person ?
4. From a security point of view, which hashing algorithm would be more robust sha1, or md5 ? Why ?
5. In a SSL connection, is it necessary for the client to send its Digital Certificate to the server ? Why ?
6. In a SSL based transaction, how does the client computer know if the certificate it has received is authentic or not ?
7. What is the factoring problem ? How is it useful in cryptography ?
8. What is a revocation certificate ?

[1]

Prepared by : Dr. Partha
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

9. Name one cryptographic system which exploits the discrete logarithm problem ?

10. What is the difference between a passive attack, and an active attack ?

11. How can you detect an attack which involves modification/tampering of the message ?

12. What is DDOS ? How can you defend yourself against DDOS ?

13. Is congruence modulo m an equivalence relation ? Justify your answer.

14. Why is PGP/GPG more secure than plain asymmetric key encryption ?

15. In the field of cyber forensics, it is often necessary to collect evidence by making a verbatim copy of the contents (directories, subdirectories, files) of the computers involved. What additional precaution should be taken to ensure that the evidence is a faithful copy of the original ?

16. CRC and hash digests achieve the same objectives : detecting messages which are corrupted in transit. What property of a hash digest distinguishes it from CRC ?

17. What is a DMZ , in the field of network security ?

18. From the point of view of security, why is it not a good idea to login as "root" in a Unix/Linux system ?

19. How does Diffie Hellman cryptography overcome the key-exchange problem ?

20. Why is it better to use a key server, rather than peer-to-peer transfer, for distribution of public keys ?

* * * * *