Kathmandu University

Information Security and Cryptography
COMP(560)

Read all the instructions, very carefully.

- Exam duration : 120 minutes
- This exam has 20 questions. Answer all questions
- All questions carry equal marks
- Your answers should be brief, precise, and to the point. You may lose marks if you give irrelevant details, or vague and ambiguous answers.
- Write legibly. You may lose marks if your answers are not legible.
- Mention the question number prominently, before you begin your answer.

Ref.: q201301a.tex[1]

1. Does the set of primes numbers P and the operation of integer multiplication (over pairwise members of P) form a group ? Why ?
2. Does the set of primes numbers P and the operation of integer addition (over pairwise members of P) form a group ? Why ?
3. If p is prime, (p-1) is not prime. True ? False ? Is there an exception to this rule ? Justify/prove your conclusion
4. Prove : Product of two consecutive numbers is even
5. True, or False ? The hash digest of a nul message is a nul sequence.
6. Explain briefly "avalanche effect" in hash digests. How does the avalanche effect of hash digests help, if passwords are stored as hash digests ?
7. How does the pre-image resistance help, in storage of passwords as hash digests ?

[1]This is an updated and revised version of the question paper administrated in Jan. 2013 at Kathmandu University.

8. How does the second pre-image resistance help, in storage of passwords as hash digests ?

9. How does asymmetric key encryption help "non-repudiation" ?

10. How does GPG/PGP use symmetric key cryptography ? Why is that helpful ?

11. Consider a star connected network with one master node (hub) and n clients (nodes).

    a. What is the minimum number of symmetric keys needed, if all the clients have to communicate securely (bi-directional) with the hub ? Mention clearly, the assumptions you have made.

    b. What is the minimum number of public keys needed, if all the clients need to communicate securely with the hub (bi-directional) using an asymmetric key protocol ? Mention clearly, the assumptions you have made.

12. Consider a mesh connected network with n clients (nodes).

    a. What is the minimum number of symmetric keys needed, if all the clients have to communicate securely (bi-directional) with each other ? Mention clearly, the assumptions you have made.

    b. What is the minimum number of public keys needed, if all the clients have to communicate securely (bi-directional) with each other using an asymmetric key protocol ? Mention clearly, the assumptions you have made.

13. What is the role of OCSP in a SSL/TLS transaction ?

14. Why is it possible in RSA to use the public key for verifying a signature made using the private key ?

15. What is the principle of DH key sharing ? Why is no key exchange involved in this method ?

16. A digital signature is a HMAC. True ? False ? Why ?

17. What is the role of digital signatures in cyber forensics ?
18. What features make IPV6 superior to IPV4 in security ?
19. Why is a web of trust not useful in PKI ?
20. Is it okay to classify Viginere cipher as a block cipher ? Why ?

* * *