Kathmandu University

Cryptography for Information Security

Duration : 120 minutes

- Answer all questions (20 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.
- Mention your branch (CS or CE) clearly, next to your name.
- Write legibly. You may lose marks if your answers are not legible.
- Mention the question number prominently, before you start your answer.

Ref.: q201307.tex

1. What is the role of modulo arithmetic in RSA cryptography ?
2. In hash digests, how is the property of pre-image resistance useful ?
3. Explain a situation where symmetric key cryptography is used in an asymmetric key algorithm.
4. Is the Vigenere cipher a block cipher ? Justify your answer.
5. Explain briefly avalanche effect in hash digests. How does the avalanche effect of hash digests help in the management of passwords ?
6. Why does digital signature use the private key of the sender ?
7. What is the principle of DH key sharing ? Why is no key exchange involved in this method ?
8. Why is OCSP more dependable than CRL in a PKI setup ?
9. How is the key length related to the robustness of a crypto system ?
10. In a relative sense, which hash digest would be considered more robust : sha1, or md5 ? Why ?

11. Why do banks and commercial establishments use digital certificates, instead of plain cryptographic tools like GPG ?

12. What is the relationship between the public key and the private key in RSA algorithm ?

13. What kind of fraud does the time-stamp in a digital signature help to avoid ?

14. In IPSEC, what cryptographic measures ensure security ?

15. What role do prime numbers play in RSA cryptography ?

16. CRC (cylic redundancy check) detects corruption of a message while in transit. What property of a hash digest distinguishes it from CRC ?

17. Give an example of discrete logarithm problem. How is it useful in cryptography ?

18. What is two-factor authentication ?

19. What is an ACL ? How is it used ?

20. What is a rootkit ?

* * *