# Information Security

# Assignment 2

***(Ques 1,2 and 3 are compulsory, do any five from remaining)***

1. Encryption is commonly used to provide data confidentiality in the Internet: when two hosts communicate, other entities in the path between the two hosts cannot read the data being sent. However, encryption on its own does not privacy of who is communicating. Although the other entities cannot read the data, they can determine which two hosts are communicating. Consider a simple view of an Internet path where client C is communicating using IPv4 with server S. There are n routers on the path. Assume a malicious user, who wants to know information about who is communicating and when, has access to one of the routers in the path (router Rm), e.g. they can capture packets on that router. Note Rm is not directly attached to the subnets of C or S.



* 1. What information can the malicious user learn about who C and S are? Consider both computer addresses and information that may identify the human user (e.g. names, locations), and explain how the malicious user may obtain that information.
  2. If Network Address Translation (NAT) is used in the subnet for C (but not for S), how does that change your answer to sub-question (a)?

One method for providing privacy in the Internet is using a Virtual Private Network (VPN). Assume client C is using a VPN server which is located on a router in the path between C and S (but not on Rm).

* 1. What information can the malicious user learn about who is communicating when C and S communicate via the VPN server?
  2. Potential disadvantages of using a VPN server include: reduced performance between C and S; required to trust the VPN server; and VPN server logs may be requested/accessed (by the malicious user). Explain each of these three potential disadvantages?

1. In using RSA, one must keep p, q, m, d private, although n and e can be public. Knowing any one of p, q, m, d is enough to break the code. Why isn’t it easy to break RSA? Can’t we just factor n to get p and q, and then compute d?
2. Suppose you receive the encrypted message 13 9 8 16 that has been enciphered using the standard MOD 26 alphabet assignment given in class and the RSA encryption method with *p* = 5 and *q* = 7 and enciphering exponent *e* = 5. Decipher this message.
3. IDS in context of Physical Security?
4. Explain strength and weakness of the following biometric systems:
   * 1. Facial Scan
     2. Retinal Scan
5. Define legal issues around the biometric systems?
6. Define the factors that should be kept in mind while designing the security metrics for an organization?
7. What makes data irreversible from hash functions, can this be used in any data security application?
8. If data can be forged even after the document being digitally signed then what exactly the Digital Signatures are being used for?
9. Implementation issues associated with firewall?