|  |
| --- |
| **Important notes:**  Although this is an open-book, open-notes exam, it is an individual exam and collaborating with others is prohibited.  Identical answers found between students will be considered as cheating and will be prosecuted per the university’s academic honesty policy.  Check the spelling and grammar before submitting your answers.  Points will be deducted from late submissions, improper subject line, and/or typos and grammatical errors. |

Your name:

**Questions and Brief Answers**

1. **(10 pts)** The security of computer systems involves multiple features, including confidentiality, data integrity, data origin integrity, availability, and non-repudiability. Suppose in certain Web-based application, the application collects customer data (d) from the individual customers who visit the Web server, and then saves the customer’s data into a database server. Explain what each of the security features means in this context. HINT: Refer to d and the Web-based application in your explanations.
2. **(10 pts)** Suppose that you have received an email from someone who claimed to be software vendor V. The vendor was trying to promote one of its software by providing a free trial version for you to use. In order to earn your trust, in that same email, the sender has attached not only the trial software (s) itself but also the vendor's digital certificate (VC). Suppose your computer tried to validate that certificate and the result was success; that is, that certificate, VC, is a valid certificate and it indeed belongs to that vendor, V. Would you trust that the software was indeed sent by that vendor? Justify your answer.
3. **(10 pts)** Describe the differences between cross-site request forgery attacks and cross-site scripting attacks. Compare their similarities and difference.
4. **(10 pts)** Describe what *input validation* means. Use SQL Injection attacks as an example to explain why input validation is essential in a Web-based application.
5. Suppose a user, Bob, has selected his RSA public key as (n = 91, e = 49), and totient(n) = 72.
   1. **(5 pts)** Explain how the totient(n) would be calculated.
   2. **(5 pts)** Show how Bob’s private key would be calculated using the *Extended Euclidian Algorithm*.