Network Lab Answer Sheet.

Please complete this answer sheet and turn it in by the due date posted in LEARN.

Part I

Question

1. (25 pts) Paste your encrypted message below:

-----BEGIN PGP MESSAGE-----

Version: GnuPG v2

hQEMAwyKQw0Mb/HmAQgArTY9/IvgXi0SVgutUnj8SQjlGLFTMXz1n+9ubAVEhO9T

znCdxwe9nCheaRQXBYs7WVuHQ0oBvvm6UY3IJN256Iv2BcqoOYza5/VdJ9YX26iy

vW7CX5to8aV0DDrAb8xlmozZd87YxCtB5A92fZdsLvZKR/KOfxuEJ7en4if7H9qM

0n8BC8/fBz359vzzNbbgfDCdtHcxMtzx86WSdKtPV9J4BXBmioCgpOXWRPU9W3nG

5TIEzksleHBOYoyqMP2oXeOwW8/93cTU2gFYEMsEImZC9/feCwsNQjQMFi9s9obu

d7hd12dMeT2eScI41qcGOdKcNkgi6W2G7zQm/vTGrdJcAXAGywOey5lfZHeUJYh3

Z96HikQ1sRjnoLLZeI3HgY2JQOc8oQRQ/hIjNPLgnjIaBwV9zKaG4Qdq681MLzVM

pGRJVnRaFdlultwsLYDNPhFx+BCxoQwjIAVdkQ0=

=HSfY

-----END PGP MESSAGE-----

|  |  |
| --- | --- |
| Question | Answer |
| 2  (5 pts) | I would use the 160 bit key because it offers the highest level of security against encrypted sensitive information being cracked. |
| Part II |  |
| 3  (10 pts) | I used Mozilla Firefox. The fields listed are certificate name, server, lifetime, and expiration date.  Certificate Name: DigiNotar Root CA, Server: none, Lifetime: permanent, Expires: March 31, 2025  Certificate Name: DigiNotar PKloverheid CA Server: none, Lifetime: permanent Expires: March 23, 2020 |
| 4  (5 pts) | It means that the connection between the server and your computer is no longer secure. |
| 5  (10 pts) | References: Amazon, Atos, and Avast Mail/Web Shield |
| Part III |  |
| 6  (5 pts) | git@gitlab.cci.drexel.edu:egm46/egm46-ci101-fall2018.git |
| 7  (10 pts) |  |
| 8  (5 pts) | The public ssh key is used to encrypt the message, which can only be decrypted using the private key. When an individual encrypts a message and sends it to someone else, they use the public key.  When the receiver decrypts the message, they use the private key. Public keys are used to encrypt only, whereas private keys can only be used to decrypt. |
| 9  (5 pts) | Command Line is quicker and easier to use because you only need the keyboard to execute commands as opposed to GUI, where you need control of the keyboard and the mouse. In the command line you are also more easily able to detect when there has been an error when interacting with your repository, unlike GUI, and conversely it is clear when you have successfully interacted with your repository, |