Homework 1

1. What C-I-A issues are in these scenarios? Instant communication; Online bank login; Ballot calculation; Online shopping; Online Map; Cloud storage; 2 more cases you can think of.

2. In the google information combination video (see the slides for lecture 1), what particular privacy leakage could it cause. Give one example. Hint: consider what Google tools you use everyday, when you use, what you search.

3. What is non-repudiation? How can you defend against repudiation in an online transaction?

4. Imagine a public service that may suffer from denial-of-service (DOS) attacks. And describe how that service will be affected by this attack.

5. What is the difference between the concepts of integrity and authenticity?

6. Decipher the following ciphertext, which was enciphered using the general Caesar Cipher: ABYU PU OVTLDVYR VU ISHJRIVHYK.  Describe what the key is for the encryption/decryption. (x offset, left/right) (Hint: you can use the caesar cipher tool on blackchamber)

7. For the models of ciphertext only attack and chosen plaintext attack , which attach model is more powerful? Why?

8. DNS service is to translate domain names into IP address, which is the only identifier computers use to locate content in the Internet. Assuming an attacker successfully launches DOS attack that drops 10% DNS requests at the DNS server side, (e.g., the URLs you type in chrome browser). In order to defend against that attack or have a perfect DNS experience (i.e., every time you type in a url, there is always good responds from DNS server), what can you do on the client side?

9. Decrypt the message in substitution cipher:

EXDWYQNEW LXAEQ EPNOE ZHXU LXAEQ EWNWQ DOAFQHEAWJ WX UASHXO WQSYOXTXGJ NTT NHQNE LQWKQQO ZQBQHNT KNJ NOB WYQ LXAEQ HAFQH. WYQ XTBQH NHQN RDEW EXDWY XZ WYQ DOAFQHEAWJ SNO LQ BQESHALQB NE N SHXEE LQWKQQO WYQ OXHWY QOB NOB WYQ LXAEQ LQOSY. WYQ HQEW XZ EXDWYQNEW LXAEQ KNE BQFQTXPQB AO WYQ TNEW WYAHWJ JQNHE KAWY EDLDHLNO-EWJTQ YXUQE. SXTDULAN FATTNGQ EDLBAFAEAXO NOB WYQ XTBQH XHQGXO WHNAT YQAGYWE KQHQ WYQ ZAHEW UNRXH PTNOOQB SXUUDOAWAQE AO EXDWYQNEW LXAEQ KAWY NO QTQUQOWNHJ NOB UABBTQ ESYXXT NTT KAWYAO KNTCAOG BAEWNOSQ ZHXU NTT YXUQE. WYQ EDLBAFAEAXO AE TXSNWQB NW WYQ AOWQHEQSWAXOE XZ AOWQHEWNWQ 84, ABNYX 21, NOB ZQBQHNT KNJ (ZXHUQH D.E. YAGYKNJ), KYASY NHQ NTT UNRXH NHWQHAQE WX GQW NOJKYQHQ AO LXAEQ. WYQ EDLBAFAEAXO, N LNEQLNTT SXUPTQM, NOB EKAUUAOG PXXTE KQHQ BQFQTXPQB NHXDOB WYQ EAUPTXW EPXHWE SXUPTQM. WYQ ZAQTBE NHQ LDATW XFQH NO XTB TNOBZATT NOB BDUP, NOB WYQ ZAQTBE NOB GHNFQT PNHCAOG TXW NTTXK HNBXO GNEQE WX QESNPQ WYHXDGY WYQ GHXDOB.