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.

   C-I-A Issues:

a) Instant communication

   Confidentiality Issue

b) Online bank login

   Confidentiality Issue

c) Ballot calculation

   Integrity Issue

d) Online shopping

   Confidentiality Issue

e) Online Map

   Integrity Issue

f) Cloud storage

   Confidentiality Issue

g) 2 more cases:

   1) Social media Login

      Confidentiality Issue

   2) Online Business

      Availability Issue: May suffer from DDoS attack

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 every day, when you use, what you search.

   Confidentiality Issue is definitely on the list. Google combination of search results from all of the google platforms which includes YouTube, google plus, google email etc which I use from day-to-day life. This not only takes away the user's anonymity on the web but further allows google to suggest the type of content to the user. Now all of these different platforms on google know and share what type content is preferred by the user. They usually defend themselves by claiming to provide better service to its multi-billion users by helping users find what they are looking for. A good example of this would be if I type in YouTube that I am a fan of huskies as I love watching those videos. Now my google plus search also knows what I like which I use at my work. This most definitely raises a confidentiality issue. Apart from this it also allows these big tech giants to run very specific targeted ads on its platform.

3. What is non-repudiation? How can you defend against repudiation in an online transaction?
   Nonrepudiation provides an assurance that the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data.
   Using digital signature to sign the document is one of the ways to defend against repudiation in an online transaction. One must use his/her private key to produce a valid digital signature, and the signature verification needs the associated public key. Like the traditional handwritten signature, a valid digital signature can assure the recipient the origin and the integrity of a message, and has received legal recognition

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.

   DoS attacks are accomplished by flooding the target with traffic or sending it information that triggers a crash. Once the attack is successful, the server may not be able to serve the legitimate users and this may affect the brand or business with losing a good amount of money and customers thus harming the brand image and also may cause the brand to go out of business in severe consequences. These attacks are hard to deal with as these are carried out from several hosts network and thus this type of attack is called DDoS which stands for Distributed Denial of Service attack.

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

   Integrity is used to make sure that nobody in between site A and B (for example) changed some parts of the shared information. -2
   Authenticity is used to make sure that you really communicate with the partner you want to.

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)

   Deciphered Text: “turn in homework on blackboard”
   Key for encryption: (7 offset, right)

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

First let's look at what each of them are:

Ciphertext only attack (COA):

a) The attacker is assumed to have access to a set of ciphertext

b) The attacker still has some knowledge to the plain text prior to cracking the key such as, the attacker might know what language the plain text could be written in by statistical distribution of characters in the plain text.

c) The attack is completely successful if the corresponding plaintexts can be deduced (extracted) or, even better, the key.

d) The ability to obtain any amount of information from the underlying ciphertext is considered a success.

Chosen plaintext attack (CPA):

a) the attacker chooses to pick a plain text and is able to encrypt the plain text message which he ends up with ciphertext message.

b) The attacker than compares the ciphertext with the result of another encryption to possibly discover the key by matching the two ciphertext.

c) If they match he can than find the key, or if they don't he can find the patterns that can lead him upto the key.

d) Either way he replicates the process with his chosen plain text to figure out what the cipher text is going to look like.

Conclusion: I consider CPA to be more powerful as the attacker has access to most information here. The attacker has *arbitrary message* (m) with *corresponding ciphertext (c),* and also has access to the encryption function which increases the chances of success on being able to come up with the key with some series of cryptic analysis.

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?

   I would simply put the Ip address of the website in my browser to the be able to access website each time to have a smooth browsing experience of that particular website.

   However, this in not practical often times as memorizing ip address is not one thing that people find it pleasing for frequently accessed websites, webpages are cached (stored) on a local computer for faster load times. Cached website and IP addresses do not always update. If the computer is trying to access a website using an outdated IP address, the request will fail. **Clearing the browser's cache** should fix the problem.

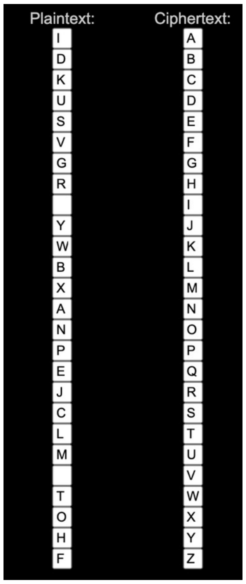
9. Decrypt the message in substitution cipher:

   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.

On the next page:

"SOUTHEAST BOISE SPANS FROM BOISE STATE UNIVERSITY TO MICRON TECHNOLOGY ALL AREAS BETWEEN FEDERAL WAY AND THE BOISE RIVER THE OLDER AREA JUST SOUTH OF THE UNIVERSITY CAN BE DESCRIBED AS A CROSS BETWEEN THE NORTH END AND THE BOISE BENCH THE REST OF SOUTHEAST BOISE WAS DEVELOPED IN THE LAST THIRTY YEARS WITH SUBURBANSTYLE HOMES COLUMBIA VILLAGE SUBDIVISION AND THE OLDER OREGON TRAIL HEIGHTS WERE THE FIRST MAJOR PLANNED COMMUNITIES IN SOUTHEAST BOISE WITH AN ELEMENTARY AND MIDDLE SCHOOL ALL WITHIN WALKING DISTANCE FROM ALL HOMES THE SUBDIVISION IS LOCATED AT THE INTERSECTIONS OF INTERSTATE IDAHO AND FEDERAL WAY FORMER US HIGHWAY WHICH ARE ALL MAJOR ARTERIES TO GET ANYWHERE IN BOISE THE SUBDIVISION A BASEBALL COMPLEX AND SWIMMING POOLS WERE DEVELOPED AROUND THE SIMPLOT SPORTS COMPLEX THE FIELDS ARE BUILT OVER AN OLD LANDFILL AND DUMP AND THE FIELDS AND GRAVEL PARKING LOT ALLOW RADON GASES TO ESCAPE THROUGH THE GROUND"

Key:



Plaintext:	Ciphertext:
I	A
D	B
K	C
U	D
S	E
V	F
G	G
R	H
	I
Y	J
W	K
B	L
X	M
A	N
N	O
P	P
E	Q
J	R
C	S
L	T
M	U
	V
T	W
O	X
H	Y
F	Z