# Lab-1-2: Security Concepts

Basic information security concepts are an essential component of understanding and learning basic security principles. This lab works in conjunction with the theory presented in this week’s class.

## Exercise-1-2-1: Assets, Threats, Vulnerabilities, Exploits, Risks

Defined below is a collection of five information security terms that we have discussed:

1. Assets: Information, data, device, or other computing/information component
2. Threats: Any circumstance with potential impact to asset
3. Threat agent: The source of the threat
4. Vulnerabilities: Flaw or weakness that may affect security
5. Exploits: The method/tool used to practically implement a vulnerability
6. Risk: The potential that a given threat will exploit vulnerabilities of an asset

**Q1.** Provide three examples of IT assets and a potential threat against each.

Answer:

Computer Hardware – Potential for theft in unmonitored areas

Afterhours access cards – Potential for theft or card loss, someone else can access the building

**Q2.** Based on what you have learned about key security terms, label each object in the diagram below:



Loss of confidential data – Risk

Hacker – Threat Agent

Stolen Data – Risk

Server – Asset

Remote code execution tool – Exploits

Unpatched Wireless access point – Vulnerability

**Q3.** During the discussion in class, we looked at some vulnerabilities and their associated exploits. Do a google search to find a vulnerability for any Microsoft operating system. Document the vulnerability including a brief summary, the Bulletin Number/CVE number, the listed severity of the vulnerability. You can also try find a corresponding exploit (NOTE: an exploit may not exist for all vulnerabilities)

Answer: CVE-2019-1359 – CVSS score of 9.3

Vulnerability exists where Windows Jet Database Engine improperly handles object in memory, potential threat for code injection

## Exercise-1-2-2: Attacks

**Q4.** Based on your answer to Q3, classify your discovered vulnerability as either a passive or an active attack (or potentially both). Also, can you think of a method in which you can perform this attack/what type of attack is it?

Answer: Both passive and active. Passive attack to find the vulnerable software – Port Scanning. Active attack to inject code

## Exercise-1-2-3: Confidentiality, Integrity, Availability (CIA)

We discussed CIA in class and watched a video by [Professor Messer](http://www.professormesser.com/security-plus/sy0-401/confidentiality-integrity-availability-and-safety/).

**Q5.** Provide one example of a technique (e.g., encryption) to achieve one of the three security mechanisms: 1) Confidentiality, 2) Integrity, or 3) Availability. Include a brief summary of how this technique can provide the security requirements needed.

Answer:

Confidentiality – Encrypting your data

Integrity – Checking MD5 value of a file

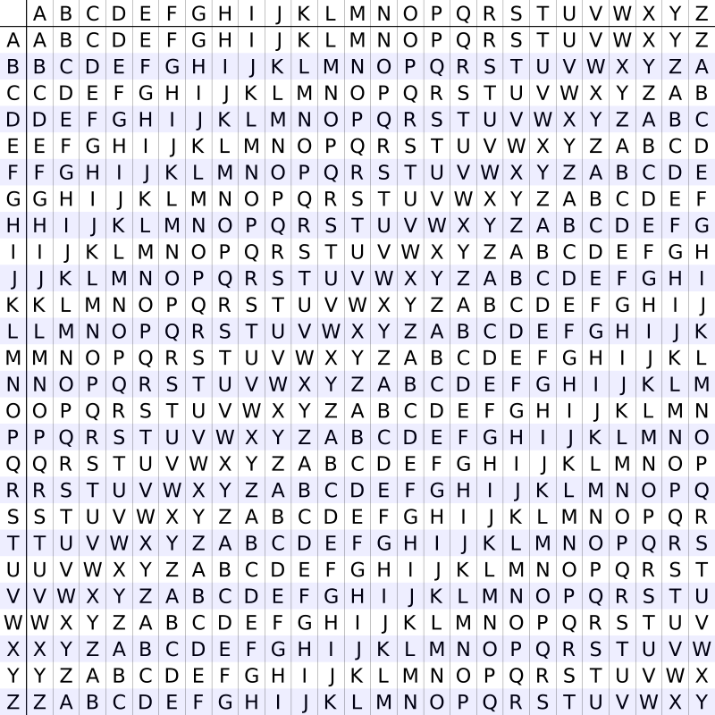
Availability

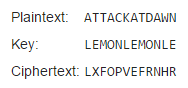
**Q6.** Non-repudiation is another type of security mechanism that we did not specifically cover in the class material. Perform some research and provide a brief summary of what non-repudiation aims to achieve with an example of where it is used.

Answer: Non-repudiation is the assurance that someone cannot deny the validity of something. Using digital signatures provides this

**Q7.** Last session we decrypted ciphertext using the Vigenere cipher (Lab 1-1, Q6.). Understanding how the cipher works, especially the use of the secret key, is very important. Describe: 1) how the secret key is used, and 2) why a polyalphabetic cipher is more resilient to attack when compared to a monoalphabetic cipher.

Answer: The key repeats. Follow the row that corresponds to the





**Q7.** Write a program to break caeser cipher in your favourite language using the chi-squared statistics method described at (<http://practicalcryptography.com/cryptanalysis/text-characterisation/chi-squared-statistic/>)

Q8. Crack the following Vigenere cipher. Use the exercise at <https://www.ti89.com/cryptotut/vigenere.htm> to understand the different steps in this process.

Writing a program will be easier following the steps.

Mvc gnxqgywa aglgghb ht Tbrbzjxg Lqfhcj wq hm dphjgws Lh Mvmfoq olw Qm Hhvl kgmv ifgoorx nkwktfw olw qxqmgrykm xrsvorbcl cd hfx fbufxgr estzgmm Mvc tsgqrbcl cd hfx Jhkck Qvvmhz bg mc ifciopx qmibxbrl dhf t pbumkcsl ahzjxuc dpxdykorhfw dphupta bb mvc Agwrjx ygr Ndnxf Lqfhcjl Ras Tbrbzjxg Lqfhcj dphupta bg wsqbulxr mc xbqnfc oq asvv tg bh bg icqlwzes mvym ekobnorxg tfc dpxdyksb hm acxh mvc obfwqlwmgg ksonwpxacghq cd hfx khgr qmfdcmwrbjc qmezczsq olw sgwtxfqbhgxg mc xlaxz bb liaa gggrbhsmwmgg tbb hm ormogg rasgk nxfqhbye ygr vopxsp umtzq Oje qvvmhz ifmzfyfg tfc rclwegsb hm rcosjhd lhswslmg tqywskbq tbb zctrckgfbd tpgewrbsq olw rasgk nxfqhbye qhqgtz tbb qgowa outfcgsql