|  |  |
| --- | --- |
| Symmetric Key Encryption | Public Key Encryption |
| Preferred technique when transferring data in bulk. | It is considered more secure because it uses two keys |
| It uses one key | Takes longer to execute |
| It is an old technique | It is newer |
| Only uses one key for encryption and decryption | Uses different keys for encryption and decryption |

1. A faraday cage is an enclosure used to block electromagnetic fields. A person need not worry about being a victim of a social engineering attack because while in this “cage” no incoming attempts from a malicious user/program will not be able to access the device (cell phone while in that cage because of the electromagnetic field.
2. Some security includes:
   1. Alteration: Person with the right tools (man in the middle for example) can intercept data and alter information sent to a server especially while students are doing an exam.
   2. Denial of service: Someone with malicious intent can deny users from using a service, especially one that pertains to final exams online. One example of this is creating traffic.
   3. Masquerading: Someone can pretend to be someone else and do the exam for you.
3. Ffdsd
4. The CIA (Confidentiality, Integrity, Availability) is a model designed to guide policies for information security.
   1. Confidentiality: it is designed to prevent sensitive information from unauthorized access attempts
   2. Integrity: purpose is to maintain the consistent, accurate and trustfulness of data during its entire lifecycle.
   3. Availability: the data should be accessible consistently and readily to the persons who should have access to it.

The AAA (Authentication, Authorization, Accounting) is a little different because it controls access to computer resources, enforces policies audits usage.

* Authentication: this is where a user provides information about who they are. Who they are determines what access will be given to them. (eg, fingerprint)
* Authorization: this follows authentication This is where a user is given permission to perform certain actions/areas on a network.
* Accounting: Keeps track of user activity while they are logged into a network.

CIA and AA are somewhat similar with each other.

1. Asa
2. Example of a strong password is one that has upper/lower case characters, special characters and numbers example: P@$$w0rd.
3. Another example of a strong password is M1ke03. This is Upper/lower case letters and numbers.
4. There are 5 characters one from upper, lower, number, special character. If you add them up you’ll get 94 characters.  
   Now if it’s a 5 character password it’ll be 945 which equals = 7,339,040,224. For a computer to get the password, it will have to process words at 1415 PW/sec
5. An access control matrix is a table that defines permissions.
   1. Row: Each row of this table is associated with a subject, which is a user, group, or system that can perform actions.
   2. Column: Each column of the table is associated with an object, which is a file, directory, document, device, resource, or any other entity for which we want to define access rights.
   3. Cell: Each cell of the table is then filled with the access rights for the associated combination of subject and object.
6. Access control list for /usr/bin/: root – r, w, e, mike – r, e, Roberto – r, e, backup – r, e  
   /admin/: root – r, w, e, backup – r, e.