|  |  |  |  |
| --- | --- | --- | --- |
|  | **Criterias** | **MD5** | **SHA1** |
|  | **Input Size** | Can vary | Can vary |
|  | **Output size** | 128 bits | 160 bits |
|  | **Initialization vector size** | 512 bits | 512 bits |
|  | **Version available in market** | MD6 is the latest version. | SHA3 is the latest version. |
| **1** | **Time taken for short msg**  “Hi” | 5.999999999999062e-06 | 7.000000000000062e-06 |
| **2** | **Time taken for moderate length msg one paragraph** “**Security Threats**  Computer systems face a number of security threats. One of the basic threats is data loss, which means that parts of a database can no longer be retrieved. This could be the result of physical damage to the storage medium (like fire or water damage), human error or hardware failures.Another security threat is unauthorized access. Many computer systems contain sensitive information, and it could be very harmful if it were to fall in the wrong hands. Imagine someone getting a hold of your social security number, date of birth, address and bank information. Getting unauthorized access to computer systems is known as hacking. Computer hackers have developed sophisticated methods to obtain data from databases, which they may use for personal gain or to harm others.A third category of security threats consists of viruses and other harmful programs. A computer virus is a computer program that can cause damage to a computer's software, hardware or data. It is referred to as a virus because it has the capability to replicate itself and hide inside other computer files.  ” | 7.000000000000062e-06 | 5.000000000001531e-06 |
| **3** | **Time taken for long length one page msg**  “Instructor: *Paul Zandbergen*  Paul has a PhD from the University of British Columbia and has taught Geographic Information Systems, statistics and computer programming for 15 years.Computer systems face a number of security threats. Learn about different approaches to system security, including firewalls, data encryption, passwords and biometrics.  Security Threats  Computer systems face a number of security threats. One of the basic threats is data loss, which means that parts of a database can no longer be retrieved. This could be the result of physical damage to the storage medium (like fire or water damage), human error or hardware failures.  Another security threat is unauthorized access. Many computer systems contain sensitive information, and it could be very harmful if it were to fall in the wrong hands. Imagine someone getting a hold of your social security number, date of birth, address and bank information. Getting unauthorized access to computer systems is known as hacking. Computer hackers have developed sophisticated methods to obtain data from databases, which they may use for personal gain or to harm others.  A third category of security threats consists of viruses and other harmful programs. A computer virus is a computer program that can cause damage to a computer's software, hardware or data. It is referred to as a virus because it has the capability to replicate itself and hide inside other computer files.  System Security  The objective of system security is the protection of information and property from theft, corruption and other types of damage, while allowing the information and property to remain accessible and productive. System security includes the development and implementation of security countermeasures. There are a number of different approaches to computer system security, including the use of a firewall, data encryption, passwords and biometrics.  Firewall  One widely used strategy to improve system security is to use a firewall. A firewall consists of software and hardware set up between an internal computer network and the Internet. A computer network manager sets up the rules for the firewall to filter out unwanted intrusions. These rules are set up in such a way that unauthorized access is much more difficult.  A system administrator can decide, for example, that only users within the firewall can access particular files, or that those outside the firewall have limited capabilities to modify the files. You can also set up a firewall for your own computer, and on many computer systems, this is built into the operating system.  Encryption  One way to keep files and data safe is to use encryption. This is often used when data is transferred over the Internet, where it could potentially be seen by others. Encryption is the process of encoding messages so that it can only be viewed by authorized individuals. Encryption is widely used in systems like e-commerce and Internet banking, where the databases contain very sensitive information. If you have made purchases online using a credit card, it is very likely that you've used encryption to do this.  Passwords  The most widely used method to prevent unauthorized access is to use passwords. A password is a string of characters used to authenticate a user to access a system. The password needs to be kept secret and is only intended for the specific user. In computer systems, each password is associated with a specific username since many individuals may be accessing the same system.  Good passwords are essential to keeping computer systems secure. Unfortunately, many computer users don't use very secure passwords, such as the name of a family member or important dates - things that would be relatively easy to guess by a hacker. One of the most widely used passwords - you guessed it - 'password.' Definitely not a good password to use.  So what makes for a strong password?   * Longer is better - A long password is much harder to break. The minimum length should be 8 characters, but many security experts have started recommending 12 characters or more. * Avoid the obvious - A string like '0123456789' is too easy for a hacker, and so is 'LaDyGaGa'. You should also avoid all words from the dictionary. * Mix it up - Use a combination of upper and lowercase and add special characters to make a password much stronger. A password like 'hybq4' is not very strong, but 'Hy%Bq&4$' is very strong.   Remembering strong passwords can be challenging. One tip from security experts is to come up with a sentence that is easy to remember and to turn that into a password by using abbreviations and substitutions. For example, 'My favorite hobby is to play tennis' could become something like Mf#Hi$2Pt%.  Regular users of computer systems have numerous user accounts. Just consider how many accounts you use on a regular basis: email, social networking sites, financial institutions, online shopping sites and so on. A regular user of various computer systems and web sites will have dozens of different accounts, each with a username and password. To make things a little bit easier on computer users, a number of different approaches have been developed. | 1.3000000000002593e-05 | 1.1000000000000593e-05 |
|  | **Comments on time taken for different length of msgs (point 1,2,3)** | More time was taken for longer message. | More time was taken for longer messages. |
| 4 | Msg “Hi” and msg “Ho”  Msg “CSS” and Msg “DSS”  (analyse one character change in input affects how many places in output ) | Change in a single input character changed 66 characters in the output. | Change in a single input character changed 39 characters in the output. |
|  | **Comments on avalanche effect** **(point 4)** |
| **5,6,7** | **Consider same messages from point 1,2, and 3 check length of message digest generated** | The output size remains the same for any length of input message. | The output size remains the same for any length of input message. |
|  | **Comments on length of msg and output** |
| **8** | **Can you find two different messages with same message digest ?** | No | No |
| **9** | **If message digest is given can you find original message** | No | No |
| **10** | **How many operations are required for birthday attack ?** | 264 | 280 |
| **11** | **Which hash function you find it strong and why?**  MD5 is faster than SHA1. But MD5 is known to have been broken, it is vulnerable to length extension attacks. SHA1 takes longer time but it is more secure than MD5. SHA1 is not yet broken. | | |