

**TEAM NUMBER : 30**

**WEB-BASED LEARNING**

**INFORMATION SECURITY LAB**

**20IC310P**

**INFORMATION AND COMMUNICATION TECHNOLOGY (I.C.T.) DIVISION-2**

**MEET SHELADIYA (19BIT076)**

**RENISH JAGANI (19BIT108)**

**VIVEK DEVRE (19BIT131)**

**Difference between Hill Cipher and Caesar Cipher with respect to Web-based Learning**

|  |  |
| --- | --- |
| **Hill Cipher** | **Caesar Cipher** |
| 1. Hill cipher is more likely to be used in securing the web based learning applications. | 1. Caesar cipher is a substitution cipher and so, it essentially offers no security in securing the web-based learning applications. |
| 1. When the Hill Cipher algorithm is used in the process of sending and receiving the information the security of the data between the client and the web server is believed to be assured. | 1. As Caesar cipher can easily be decrypted (substitution cipher), the process of sending and receiving the data between the client and the web server is less secure and can be hacked easily. |
| 1. Because of its quick encryption and decryption speeds, Hill Cipher is highly recommended for usage in text-based material (Tutorials and guides for the students). | 1. Caesar cipher is comparatively slower than the Hill cipher and thus it is not recommended for usage in text-based materials. |
| 1. Hill cipher is excellent for protecting data being transmitted over an open network of the web-based learning applications. | 1. As Caesar cipher can be easily cracked in very few number of trials by shifting the characters of the encrypted text as compared to other advanced ciphers (such as Hill cipher), data protection cannot be assured using it over an open network. |
| 1. Users of data delivery services no longer have to be concerned about attackers attempting to breach security systems and steal data thanks to hill cipher algorithm. | 1. Such important security systems do not use easily hackable ciphers like Caesar cipher. |
| 1. Hill cipher assures the security between the application server and the database server of the web-based learning applications. | 1. Inter-server security is not assured by easily hackable ciphers like Caesar cipher. |
| 1. The cyber-attack on web-based server (Hill cipher securing it) requires full search over all the keys possible. Cracking this cipher using brute force approach will require to test all the p raised to n square matrices (p is a prime number). | 1. It will require only 26 combinations to decrypt the used Caesar cipher using brute force approach. |

|  |  |
| --- | --- |
| 1. To send the sensitive credentials of the users the web server needs to send that data to database server for verification. Usually both the servers are on the same trusted network but it is highly recommended to use a Hill Cipher based encryption to encrypt their communication. | 1. The Caesar cipher can be easily broken by analyzing the frequency of the letters (counting the number of each letter makes it easy to guess the frequent letters). Hence, it cannot be used in protecting the sensitive credentials. |
| 1. Many websites send their sensitive data in clear text, but if some hacker is able to compromise the web server he will be able to view the user’s important credentials in that clear text. Hill cipher based encryption can be used to secure these clear texts. | 1. Substitution ciphers such as Caesar cipher are not at all recommended in securing such sensitive data in clear texts. |
| 1. It is always recommended by the web-based learning applications to ensure that their data is encrypted end to end from the browser to the database server or application server. | 1. Caesar cipher does not provide end to end encryption. |