|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Nome: Pedro Gabriel Garcia Ribeiro Balestra | | |  |  | Matrícula:1551 |  |
| Curso: GEC |  |  | Período: P8 |  | Matéria: T106 |  |

**Tarefa 3**

1. É a propriedade que garante que a informação não seja violada ou corrompida, durante a transferência, mantendo a todas as características da mensagem original. Com ela temos a garantia de que os dados não sejam indevidamente alterados. Os principais algoritmos de integridade são SHA-1, SHA-2, MD5, SHA-256, SHA-512. Onde o MD5 calcula resumo da mensagem de 128-bits em um processo de 4 etapas, enquanto o SHA-1 calcula resumo da mensagem de 160-bits.
2. Uma colisão Hash é quando o código gerado é igual a de outra mensagem, já que a função hash é formada a partir da entrada de uma mensagem. Um exemplo onde pode ocorrer uma colisão Hash são em operações bancárias, onde golpistas podem tirar proveito da situação, tendo que 2 mensagens podem ter o mesmo hash. A probabilidade de ocorrer colisão no algoritmo SHA-256 é de enquanto no algoritmo SHA-512 .

Fonte: <https://pt.wikipedia.org/wiki/SHA-2>