**Bài tập lab 1 - Hash Functions**

**Bài 1:**

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Từ khóa** | **Thuật toán băm** | **Mã băm** |
|  |  |  |  |
| 1 | cybersecurity | RIPEMD | a9b3bf6c13392c8978a762f962b78fae2e2966bd |
|  |  |  |  |
| 2 | cryptography | SHA256 | e06554818e902b4ba339f066967c0000da3fcda4fd7eb4ef89c124fa78bda419 |
|  |  |  |  |
| 3 | visual studio code | SHA1 | 79af8c85a61f665839503896580a37004d7eaa7e |
|  |  |  |  |
| 4 | communication link | MD5 | 26f27b04cfbad97705d0ac111883d6d6 |
|  |  |  |  |
| 5 | Alice | SHA512 | 299403b3d6b5c6244fc0ec6f278cb8c233734f0c156c6b8c214341fd6f8f7c781b9b2a137a09329032b9d58e8a37060690521a7d93631d43699efce8106085c9 |
|  |  |  |  |

**Bài 2:** Sự khác nhau của 5 thuật toán mã băm MD5, SHA1, SHA256, SHA512, RIPEMD

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Thuật toán** | **Kích thước**  **đầu ra** | **Kích thước trạng thái trong** | **Kích thước khối** | **Độ dài** | **Kích thước world** | **Xung đột** |
| MD5 | 128 | 128 | 512 | 64 | 32 | Có |
| SHA1 | 160 | 160 | 512 | 64 | 32 | Có lỗi |
| SHA256 | 256/224 | 256 | 512 | 64 | 32 | Không |
| SHA512 | 512/384 | 512 | 1024 | 128 | 64 | Không |
| RIPEMD | 128 | 128 | 512 | 64 | 32 | Có |