|  |
| --- |
| Bước 1: Lấy plaintext và chia nó thành một mảng gồm các mã ASCII của các ký tự. |
|  |
| Bước 2: Chuyển đổi mã ASCII sang mã nhị phân.  Bước 3: Thêm các số không vào phía trước mỗi số cho đến khi chúng dài 8 bit. |
|  |
| Bước 4: Ghép thành một mảng và thêm ‘1’ cuối mảng. |
|  |
| Bước 5: Chèn message nhị phân bằng các số không cho đến khi độ dài của nó là 512 mod 448. |
|  |
| Bước 6: Lấy mảng mã ASCII 8 bit nhị phân từ bước 3, lấy độ dài của nó ở dạng nhị phân.  Bước 7: Pad bằng các số không cho đến khi nó còn 64 ký tự.  Bước 8: Nối vào message nhị phân đã tạo trước đó của bạn từ bước 5. |
|  |
| Bước 9: Chia message thành một mảng 'chunk' gồm 512 ký tự.  Bước 10: Chia từng chunk thành một mảng con gồm 16 'words' 32 bit. |
|  |
| Bước 11: Lặp qua từng mảng 'chunk' gồm 16 'words' có 32 bit và mở rộng mỗi mảng thành 80 'words' bằng cách sử dụng các phép toán bitwise. |
|  |
| Bước 12: |
|  |
| Bước 13: |
|  |
| Bước 14:  Bước 15: |
|  |
| Kết quả |
|  |