**Mã hóa/ Giải mã Đối xứng DES và AES**

1. **Mã hóa đối xứng cơ bản – Mã hóa Ceasar:**

* Dùng một khóa chung cho cả mã hóa lẫn giải mã bằng cơ chế dịch xoay vòng ký tự qua lại một khoảng cách (shift) cho trước. Gọi M là số ký tự của bảng ký tự đuôc dùng.
* Gọi scrC là ký tự ban đầu, encodedC là ký tự đã mã hóa. Hàm tính toán của mã hóa đối xứng như sau trong đó mod là phép toán modulo (lấy thương số dương của phép chia nguyên):

|  |  |
| --- | --- |
| ***Mã hóa*** | Code (encodedC) = ( Code(srcC) + key) mod M |
| ***Giải mã*** | Code (srcC) = ( Code(encodedC) - key) mod M |

* Sự khác biệt giữa toán từ % trong ngôn ngữ lập trình và phép toán mod trong số học:

|  |  |
| --- | --- |
| **Toán tử %** | **Phép toán modulo (mod)** |
| 5%10 🡪 5  - 5%10 🡪 -5 | 5 mod 10 🡪 5, thương số 0, dư số 5  -5 mod 10 🡪 5, thương số -1 , dư số 5 |

Vì mã của ký tự là số nguyên dương nên cần phải hiệu chỉnh ách dùng toán tữ % để cho kết quả giống phép toán modulo của số học:  **x%M** nên được chuyển thành **(x+M)%M**.

***Thí dụ***: Với key=shift =3 và bảng mã ASCII, M = 256

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Dữ liệu nguổn** | |  | **Dữ liệu đã mã hóa** | |
| Ký tự | Mã ASCII |  | Mã ASCII | Ký tự |
| A | 65 | 🡪 | (65 + 3 + 256 )%256 🡪 68 | D |
| A | (68-3+256)%256 🡪 65 | 🡨 | 68 | D |

* Mã hóa đối xứng không an toàn vì hacker có thể thay đổi lần lượt các khóa để dò tìm key đã dùng ( phương pháp vét cạn, Brute Force). Dữ liệu nguồn thông thường là những dữ liệu con người có thể đọc được bởi nên thông qua cơ chế dò tìm sẽ lần lượt thay đổi khóa cho đến khi hacker đọc được dữ liệu nghĩa là họ đã bẻ khóa thánh công. Việc dò tìm này dĩ nhiên là tốn nhiều thời gian nhưng máy tính ngày nay đã chạy rất nhanh.
* Để khắc phục yếu điểm của mã hóa đối xứng cơ bản là dễ bị bẻ khóa, một số kỹ thuật giúp tăng cưởng tính bảo mật của mã hóa đối xứng có thể áp dụng:

***Thí dụ:*** Dùng mảng keys = {5, 9, 8}

|  |  |
| --- | --- |
| Dữ liệu nguồn | ABCDEFGH |
| Dữ liệu đã mã hóa | (A+5)(B+9)(C+8) (D+5)(E+9)(F+8) (G+5)(H+9) |

**Thí dụ:** Dùng chuỗi keys = ILOVE

|  |  |
| --- | --- |
| Dữ liệu nguồn | ABCDEFGH |
| Dữ liệu đã mã hóa | (A+I)(B+L)(C+O) (D+V)(E+E)(F+I) (G+L)(H+O) |

**Thí dụ:** Dùng muối là ký tự @ đặt vào sau nhóm 3 ở chuỗi nguồn rồi mới mã hóa.

|  |  |
| --- | --- |
| Dữ liệu nguồn | ABCDEFGHIJKLMN |
| Dữ liệu nguồn đã thêm muối | ABC@DEF@GHI@JKL@MN |

1. **Mã hóa đối xứng DES và AES**

* Mã hóa bằng phép toán XOR: Mã hóa và giải mã cúng dùng một khóa. Một thí dụ dùng 8 bit

|  |  |
| --- | --- |
| Dữ liệu ban đầu 8 bit | 10011101 |
| Khóa 8 bit | 01101001 |
| Dữ liệu đã má hóa 8 bit | 11110100 |
| Khóa 8 bit | 01101001 |
| Dữ liệu đã giải mã 8 bit | 10011101 |

* Bảng mã Base64 là bảng mã 6 bit có thể mô tả 64 ký tự a..z (26 ký tự), A..Z (26), 0..9 (10) ký tự + và /. Base64 được dùng làm bảng mã trung gian trong chuẩn mã hóa DES và AES. Ngày nay Base64 được dùng trong truyền thông hình ảnh, âm thanh.
* Mã hóa DES (Data Encryption Standard) và AES (Advanced Encryption Standard) là các dạng mã hóa đối xứng nhưng phức tạp hơn mã hóa Ceasar rất nhiều nhằm gây khó khăn cho những hacker. Những biến thể có thể là: khoảng cách dịch chuyển thay đổi (dùng hẳn một bộ khóa, DES dùng 8 khóa, AES dùng nhiều khóa hơn), mã hóa nhiều lần với các bộ khóa khác nhau.

**Đặc điểm của DES – Data Encryption Standard**

* DES sử dụng chung một giải thuật cho mã hóa và giải mã.
* Dùng một bảng khóa chung gồm 8 khóa. Mỗi khóa có độ dài 64 bít, trong đó thực sử dụng 56 bít còn 8 bít dùng cho kiểm tra chẵn lẻ (parity bits). Các khóa trong bảng được hoán vị vòng tròn trong qua trình mã hóa và giải mã nhằm tăng tính bí mật để khó đoán.
* Dữ liệu đầu vào được chia thành từng khối 64 bit rồi thực hiện phép toán (thường là XOR) với một khóa tương tứng đã chọn trong bảng khóa để cho 64 bit đầu ra.
* Hiện nay, mã hóa DES không được xem là phương pháp mã hóa an toàn vỉ không gian khóa nhỏ, 56 bits, nên dễ dò tìm bằng kỹ thuật vét cạn.

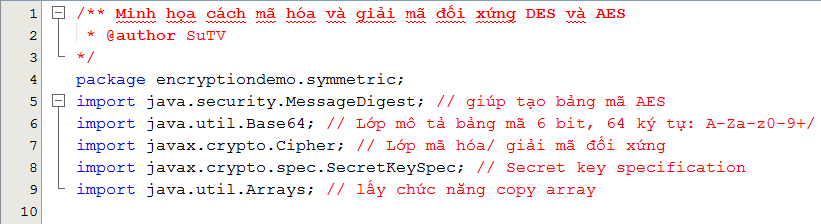
**Đặc điểm của AES- Advanced Encryption Standard**

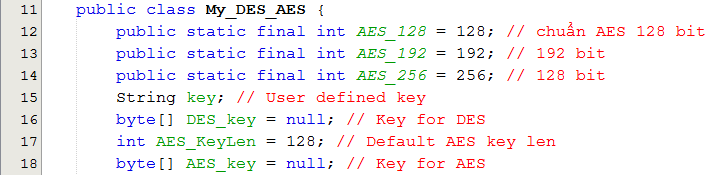
* Độ dài khóa có thể là 128 bít (16 bytes), 192 bít (24 bytes) hay 256 bít (32 bytes) tương ứng với các chuẩn được đặt tên là AES-128, AES-192 và AES-256.
* Để tăng độ khó, các khóa được hoán vị (permutation). Một khối dữ liệu được mã hóa nhiều vòng (round) trước khi kết thúc một khối. Mỗi vòng dùng một khóa riêng. AES-128 sử dụng 10 vòng, AES-192: 12 vòng và AES-256: 14 vòng.
* AES có thuật toán phức tạp hơn DES nên được đánh giá là an toàn hơn.
* Tham khảo thêm:

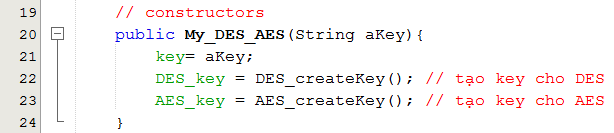
<https://en.wikipedia.org/wiki/Advanced_Encryption_Standard>

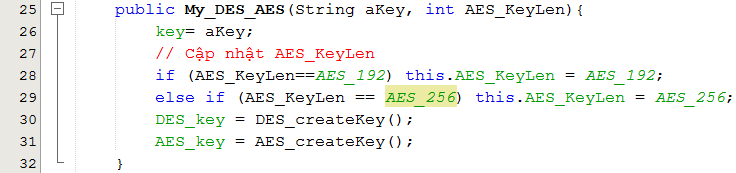
<https://en.wikipedia.org/wiki/Advanced_Encryption_Standard_process>

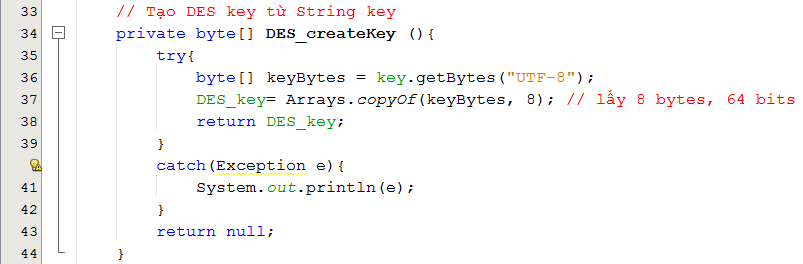
**Code minh họa**

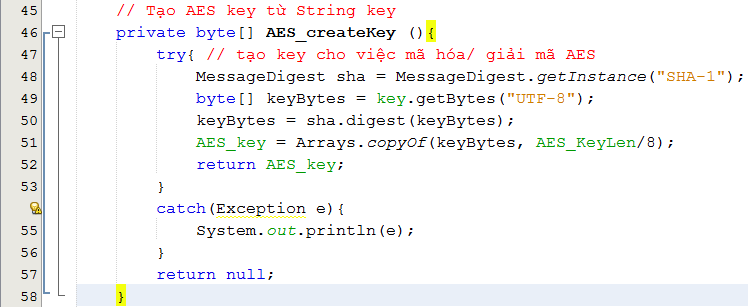


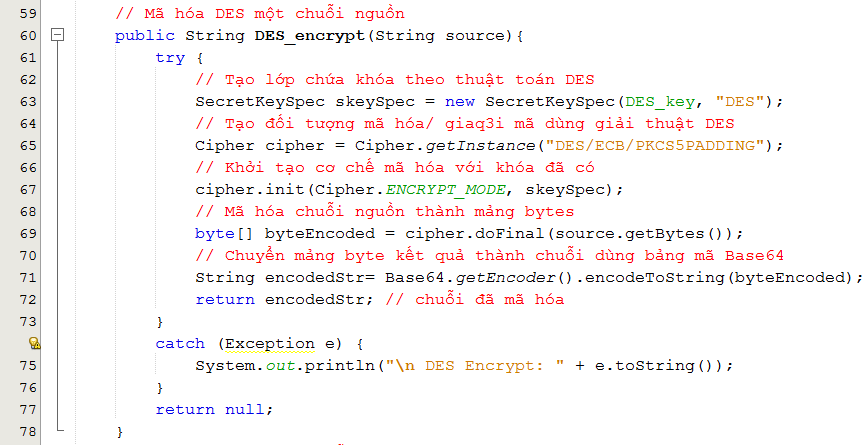


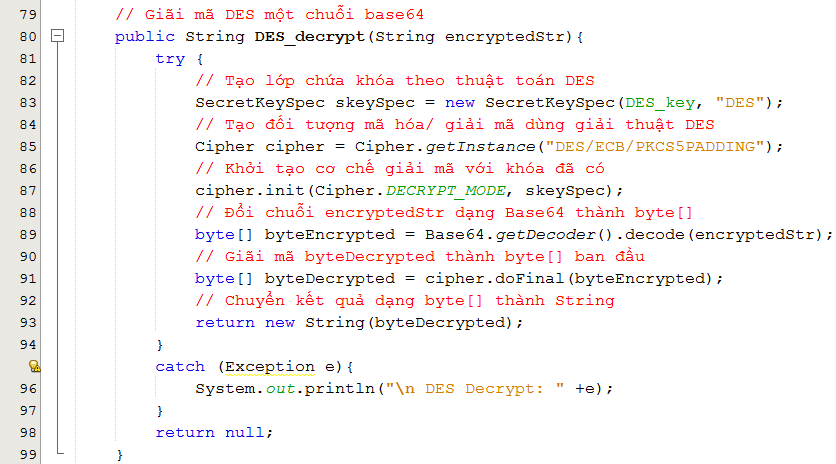


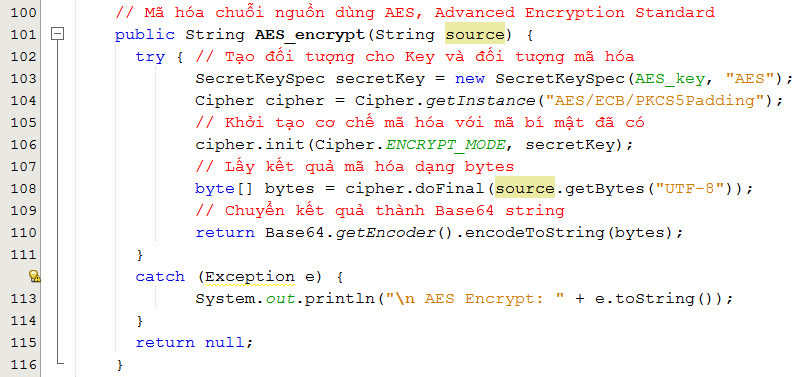


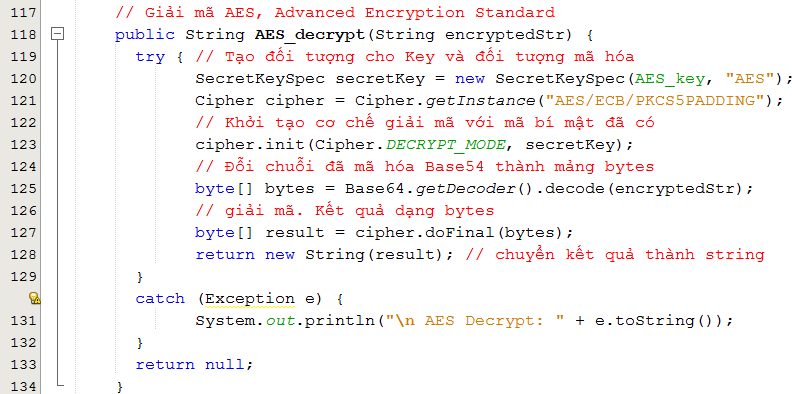


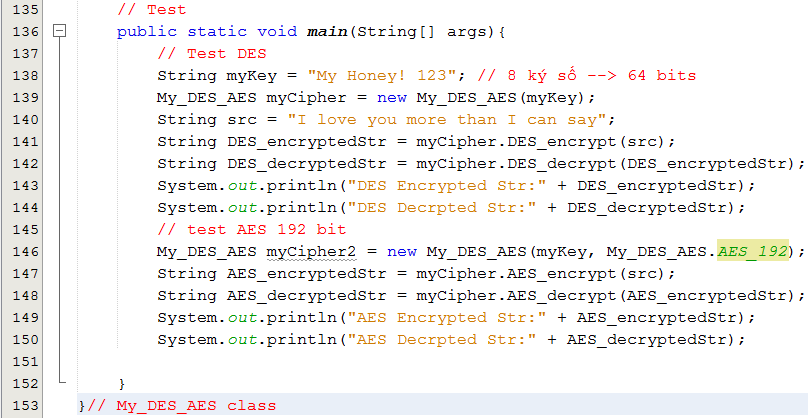












**Kết quả kiểm thử:**

