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

**Mã hóa đối xứng:**

* Dùng một khóa chung cho cả mã hóa lẫn giải mã
* Mã hóa Ceasar là một dãng mã hóa đối xứng thông qua khóa là khoảng cách dịch chuyển. Nếu lúc mã hóa dịch mỗi ký tự tới n vị trí thì khi giải mã sẽ dịch lùi n vị trí. Khóa của mã hóa Ceasar là n.
* Mã hóa DES (Data Encryption Standard) và AES (Advanced Encryption Standard) là các dạng mã hóa đối xứng. Các dạng mã hóa này phức tạp hơn mã hóa Ceasar.

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

* Dùng một khóa chung cho cả mã hóa và giải mã
* Là dạng mã hóa khối, kích thước khối vào 64 bít: (khối 64 bit + khóa) 🡪 Khối dữ liệu đã mã hóa
* Khóa có độ dài 64 bít, trong đó thực sử dụng 56 bít còn 8 bít dùng cho kiểm tra chẵn lẻ (parity bits)
* DES sử dụng chung một giải thuật cho mã hóa và giải mã.
* Tham khảo cơ chế làm việc của DES: https://en.wikipedia.org/wiki/Data\_Encryption\_Standard
* 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 (giải thuật vét cạn Bruth Force). Hơn nữa các hệ thống máy tính ngày càng mạng và nhanh.

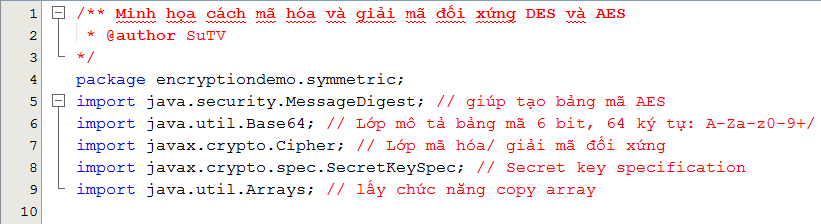
**Đặc điểm của AES- Advanced Encryption Standard**

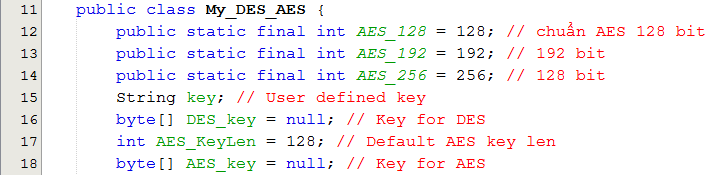
* Độ dài khóa có thể là 128 bít (16 bytes), 192 bít (24 bytes) hay 256 bít (32 bytes) tương ứng dọi là AES-128, AES-192 và AES-256.
* AES-128 sử dụng 10 vòng lặp để mã hóa, (round), AES-192: 12 vòng và AES-256: 14 vòng.
* AES có thuật toán phức tạp hơn DES nên được đánh giá là an toàn hơn.
* Tham khảo thêm:

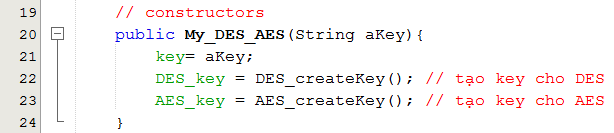
<https://en.wikipedia.org/wiki/Advanced_Encryption_Standard>

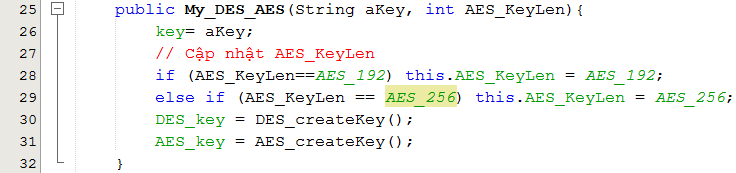
<https://en.wikipedia.org/wiki/Advanced_Encryption_Standard_process>

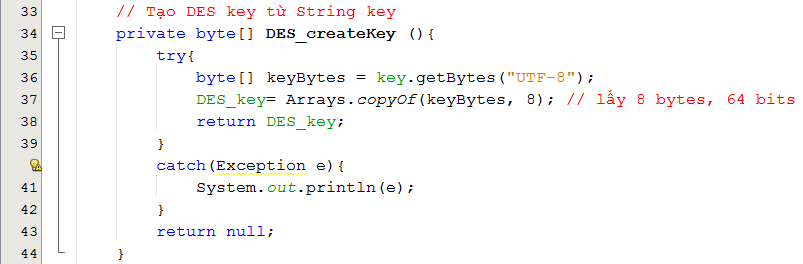
**Code minh họa**

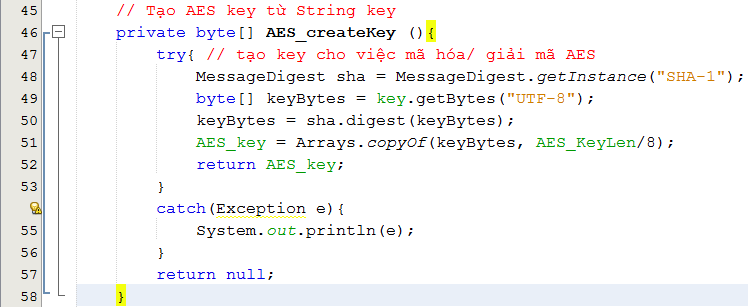


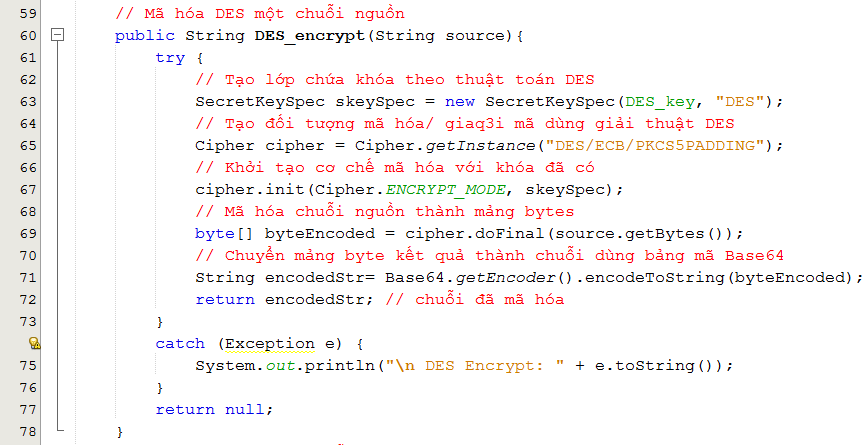


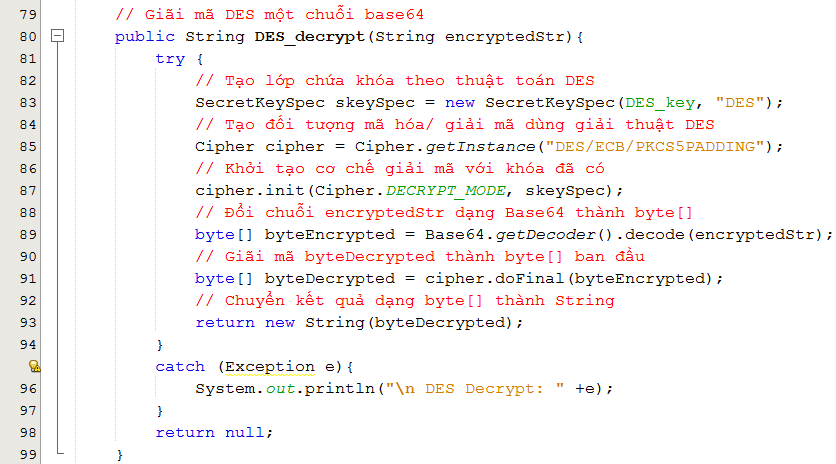


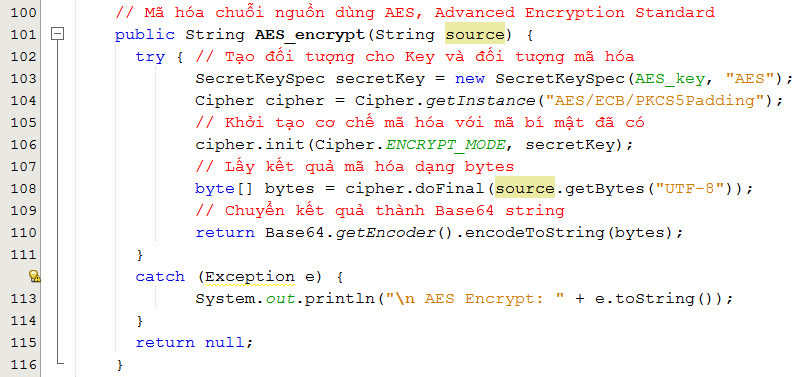


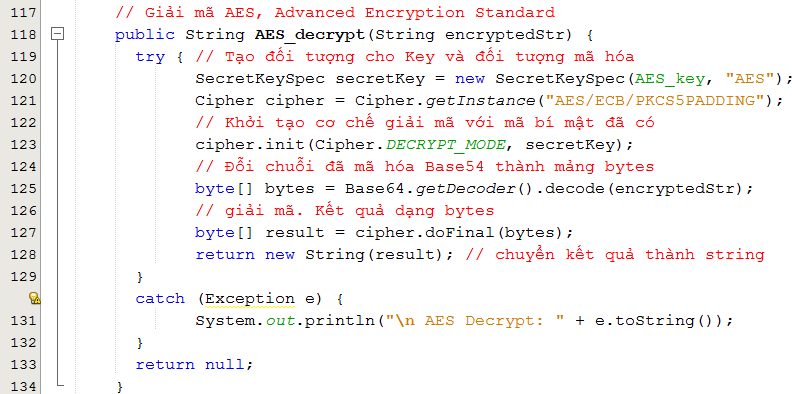


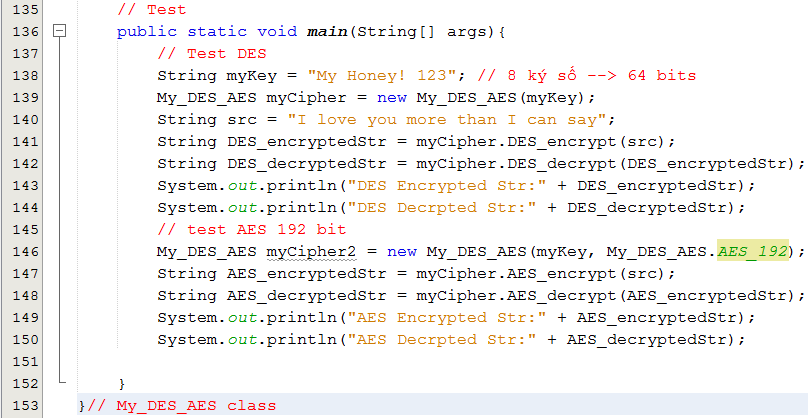












**Kết quả kiểm thử:**

