Bài tập lập trình 2
Sử dụng mã khối

Bạn hãy cài đặt hai sơ đồ mã hoá và giải mã:

1. AES với CBC mode
2. và AES với Counter mode (CTR).

Cả hai sơ đồ đều dùng IV ngẫu nhiên 16-byte. Với CBC ta dùng PKCS#7 padding (như mô tả trong slides). Bạn có thể viết lại hàm AES hoặc dùng lại mã nguồn cài đặt AES hoặc dùng thư viện có sẵn.

Bạn phải viết một file README mô tả ngắn gọn chương trình của bạn và cách cài đặt và thư viện sử dụng.

Bạn nên so sánh chương trình của mình với thư viện pycrypto để kiểm tra hiệu năng của chương trình.