Bài tập

Một lập trình viên muốn sử dụng CBC để đảm bảo toàn vẹn và bí mật cho các gói tin trên mạng. Chị ta gắn một khối toàn bit 0 vào cuối của bản rõ $x_1 \| \cdots \| x_n$ và mã hóa với CBC. Khi nhận được bản mã, chị ta sẽ giải mã và kiểm tra các bít thừa xem có phải toàn 0 không. Liệu cách này có đảm bảo tính toàn vẹn của thông điệp gửi hay không?