GIAO THỨC AN TOÀN MẠNG

BÀI 1

Các thành phần của mạng máy tính: End point (Thiết bị đầu cuối), Môi trường truyền dẫn, Giao thức

?1 OWASP (2017-2021)

Chế độ hoạt động của mã khối

Mã khối có nhiều chế độ làm việc khác nhau: ECB, CBC, OFB, CDB, CTR, GCM,…

Một số chế độ là thuần tuý mã khối: ECB, CBC, CTS

Một số chế độ là tương tự như mã dòng: OFB CFB, CTR…

?2 Padding Oracle

?3 Chữ ký số dùng để làm gì

Dịch vụ an toàn: bí mật, xác thực, toàn vẹn, sẵn sàng, chống chối bỏ

Kỹ thuật an toàn: ngăn cản vật lý, định danh, cấp quyền, xác thực, mã hoá

Giao thức an toàn mạng: là 1 giao thức mật mã được sử dụng để bảo vệ dữ liệu trên máy tính và dữ liệu trên đường truyền