A white text with black text

Description automatically generated

Câu 1:

Kiểm soát dịch vụ: Xác định dịch vụ truy nhập, hướng ra ,vào

Kiếm soát hướng: điều khiển hướng đc phép đi của các gói tin của mỗi dịch vụ

Kiểm soát người dung: Xác định người nào được truyền nhập

(Thường là những người trong nội bộ mạng)

Kiểm soát hành vi: Kiểm soát việc sử dụng các dịch vụ cụ thể.  
Vd tường lửa có thể lọc loại bỏ thư rác,hạn chế truy nhập đến 1 bộ phận thông tin của máy chủ

Hạn Chế:

Không chống các phần mềm không đi qua nó

Không chống các cuộc tấn công dữ liệu hoặc tấn công lỗ hổng phẩn mềm

Không chống lại được hiểm hoạ bên trong mạng nội bộ

Không ngăn các chương trình,file nhiễm virus,phần mềm độc hại

Câu 2:

a)

Beta = Mod p = Mod 107 = 78

Kp = (alpha,beta,p) = (5,78,107)

Ks = a = 83

b)

C1 = Mod p = Mod 107 = 16

C2 = M \* Mod p = 150 \* Mod 107

150 Mod 107 \* Mod 107 = (43 \* 13) Mod 107 = 24

C = (C1,C2) = (16,24)

CT Giải Mã:

M = (C2 \* ) Mod P Với Mod p = Mod p

= (C2 Mod p \* Mod P) Mod P

= (C2 Mod p \* Mod p) Mod P

= (24 Mod 107 \* Mod 107) Mod 107

= (24 \* Mod 107) Mod 107

= (24 \* 33) Mod 107

= 43

VÌ M nằm trong khoảng 0<=M<P nên M = 150 mod 107 = 43