A white paper with black text

Description automatically generated

Câu 1:

* Cơ sở dữ liệu chữ kí : chứa các mẫu tấn công và dấu hiệu của các tấn công đã biết
* Khi dữ liệu được thu thập từ nguồn chuyển đến bộ phân tích của hệ thống
* Bộ phân tích sẽ so sánh dữ liệu với cơ sở dữ liệu chữ kí
* Nếu trùng khớp , hệ thống xác định đây là một cuộc tấn công và tiến hành cảnh báo ngăn chặn tới ng dùng
* IDS ghi lại sự kiện và gửi cảnh báo
* IPS: ngăn chặn bằng cách chặn lưu lượng …

Câu 2:

a)

N = p \* q = 31 \* 41 = 1271

P(N) = (p-1)(q-1) = 30 \* 40 = 1200

d = Mod P(N) = Mod 1200

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| A | B | R | Q | Y0 | Y1 | Y |
| 1200 | 379 | 63 | 3 | 0 | 1 | -3 |
| 379 | 63 | 1 | 6 | 1 | -3 | 19 |
| 63 | 1 | 0 |  |  |  |  |

d = 19

Kp = (N,e) = (1271,379)

Ks = (d,p,q) = (19,31,41)

b)

M’ = Mod N = Mod 1271 = 60 = M => Chữ ký hợp lệ