Câu 1:

Trong mật mã học, **one-time pad** là một hệ thống trong đó một khóa riêng được tạo ngẫu nhiên và được sử dụng một lần duy nhất để mã hóa một thông điệp sau đó được giải mã bởi người nhận bằng chính khóa đó.

Tin nhắn được mã hóa với các **Khóa** dựa trên sự ngẫu nhiên có lợi thế là về lý thuyết là không có cách nào để "phá vỡ các mã" bằng cách phân tích .Tuy nhiên ,việc giải mã đòi hỏi người nhận phải sử dụng cùng chìa khóa với người mã hóa điều này đặt ra vấn đề -> Làm cách nào để chìa khóa đến bên giải mã một cách an toàn ? Hoặc làm thế nào để cho cả hai khóa (người mã hóa và người nhận) phải được an toàn ? Trên internet , những khó khăn trong việc kiểm soát tính an toàn của khóa bị mật đã dẫn đến sự ra đời của việc sử dụng khóa công khai!

Câu 2:RSA

(e, N) is the *public RSA key.*
(d, N) is the *private key.*

Thuật toán RSA được đề xuất bởi Rivest, Shamir và Adleman.
Gọi p và q là hai số nguyên tố lớn ngẫu nhiên phân biệt.
Modun n là tích của hai số nguyên tố này $n = pq$
Hàm phi Euler (Euler's totient function) của n cho bởi:
$\varphi(n) = (p - 1)(q - 1)$
Chọn một số $1<e<\varphi(n)$ sao cho:
$gcd(e, \varphi(n)) = 1$
và tính d với công thức:
$d = e^{-1} mod\ \varphi(n)$
Việc mã hóa được thực hiện bằng cách tính:

$$C = M^e \pmod n$$

với M là plaintext, C là ciphertext tương ứng của M.
Từ C, M được tính bằng công thức:

$$M = C^d \pmod n$$

Câu 3: Chức năng firewall:

- Packet filter.
- circuit-level proxy.
- application-level proxy.

Câu 4: So sánh tunnel mode và transport mode.

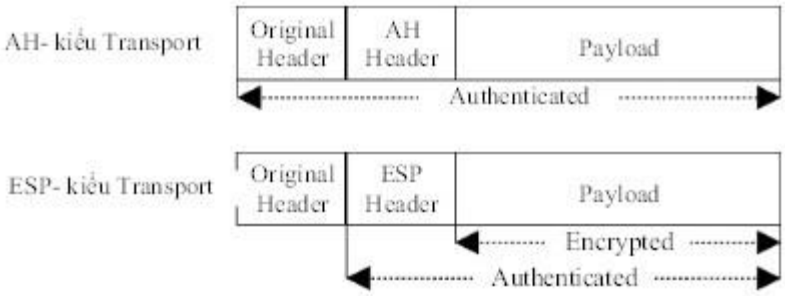
IPSec có hai kiểu cung cấp nhận thực và mã hóa mức cao để thực hiện đóng gói thông tin, đó là Transport mode (truyền tải) và Tunnel mode (đường ngầm).

1. Transport mode:

Trong mode này các dữ liệu giao tiếp với các gói tin được mã hóa/ xácthực. Trong quá trình routing, IP header không bị chỉnh sửa hay mã hóa, nhưng khi chế độ Authentication header của Ipsec được sử dụng thì địa chỉ IP cũng sẽ được mã hóa bằng cách chia nhỏ thành các gói tin riêng rẽ và độc lập (Hash).

Transport và Application layer thường được bảo mật bằng hàm Hash, chúng không thể chỉnh sửa.

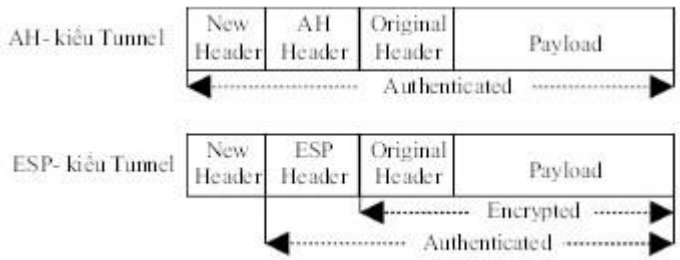
Transport mode được sử dụng trong giao tiếp host – to – host.



Gói tin IP ở Transport mode

2. Tunnel mode:

Trong Tunnel mode, toàn bộ gói IP (bao gồm cả data và header) sẽ được mã hóa và xác thực.Toàn bộ gói IP được định dạng thành một IP packet khác trong qúa trình routing của router.Tunnel mode được sử dụng trong giao tiếp network – to – network. Hoặc host – to – network và host – to – host trên internet.Do IPSec hoạt động ở lớp Network nên nó không phụ thuộc vào lớp Data Link như các giao thức dùng trong VPN khác như L2TP, PPTP.



Gói tin IP ở Tunnel mode