INDIQUE CLARAMENTE EL GRUPO DE ALGORITMOS QUE ANALIZA, N° DE PADRÓN Y NOMBRE Y APELLIDO en cada hoja.
Cada uno debe resolver la práctica contestando las preguntas y cada uno debe entregar la práctica cuando termina la clase aunque no esté terminada. La clase siguiente entrega lo que falta.

(Si Ud. faltó a clase (13/4/2004), debe resolver los algoritmos correspondientes al grupo 4 individualmente), del capitulo 8 de Computer Networks 4° Edición de A. Tanenbaum.

Utilizando los tres algoritmos del grupo que se le asigne resuelva para cada uno:

1. Haga un gráfico del algoritmo y del uso de las claves.
2. Explique brevemente como se intercambian las claves.
3. Haga un ejemplo de como se hace una transferencia de un mensaje y explique como lo transforma el algoritmo. Explique como se revierte el proceso en la otra punta.
4. Explique si el algoritmo es de clave secreta o clave pública.
5. Solamente para los algoritmos de clave pública:
   i. Explique que requisitos tiene que cumplir un algoritmo de clave pública para que se pueda usar como firma digital.
   ii. Haga un diagrama de firma digital y marque las diferencias con el de clave pública.

(El tercer algoritmo se resuelve luego de haber discutido en clase, los dos anteriores.)

Grupo	***Algoritmo 1***	***Algoritmo 2***	***Algoritmo 3***
1	Sustitución	DES	PGP
2	Transposición	AES	KERBEROS
3	One Time Pads	SHA-1	Diffie-Hellman
4	Quantum Cryptography	RSA	SSL