Define los siguientes conceptos (0,5 pto por cada una):

Algoritmo criptográfico simétrico: algoritmo el cual usa la misma clave para encriptar y desencriptar los mensajes del emisor y receptor.

Ataque de cumpleaños: es más facil encontrar un par identicos que una pareja para un individuo dado

Corte inconsistente: corte tal que no contiene los sucesos que sucedieron antes que él. (consistente lo contrario)

Sistema distribuido síncrono: sistema en el cual no estan definidos los límites de tiempo máximo y mínimo y no se sabe los límites de deriva de cada reloj

Tiempo UTC (Universal Time Coordinated): tiempo universal coordinado, para comprobar y sincronizar el tiempo, sus señales van por tierra y satelites. Se basa en el tiempo atómico y se calibra con el astronómico.

Función de resumen seguro: función Hash H la cual se computa con (h: H(M)). Dado M facil cálculo de h, Dado h difícil calculo de M. Dado M, difícil encontrar M' tal que H(M) = H(M') → funcion dispersión un sentido

Reloj de Lamport: Se sincronizan eventos según de "suceden antes" (No se sincronizan relojes)

Sincronización de relojes interno: 2 relojes coordinan sus tiempos entre sí

Tasa de deriva: diferencia en la que un reloj deriva del tiempo perfecto.

Reloj correcto: reloj H del cual se conoce su tasa de deriva

corte de la ejecución del sistema: transiciones entre estados globales

Certificados: sentencia que sirve de credencial o autenticación firmada por un principal

Evento: acción que ha ocurrido al ejecutarse un proceso

reloj defectuoso: el cual no cumple las condiciones de corrección

fallo de ruptura: el reloj no emite tics o se para

fallo arbitrario: cualquier otro fallo