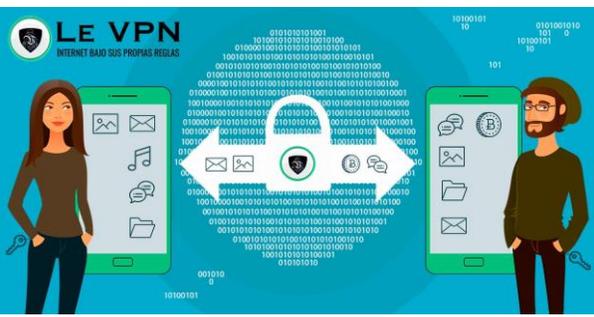


UNIVERSIDAD DEL SURESTE

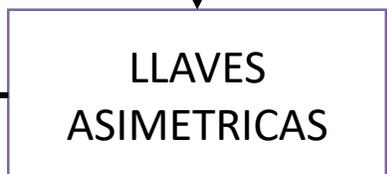


- ❖ CARRERA: INGENIERIA EN SISTEMAS COMPUTACIONALES.
- ❖ SEMESTRE: 7°- CUATRIMESTRE.
- ❖ MODULO: 1 MODULO.
- ❖ DOCENTE: EDUARDO GENNER ESCALANTE CRUZ.
- ❖ MATERIA: REDES DE COMPUTADORAS III.
- ❖ TEMA: REPASO DE REDES DE COMPUTADORAS III.
- ❖ ALUMNA: LAURA DENIS TON HERNANDEZ.
- ❖ FECHA: 18/10/2020.

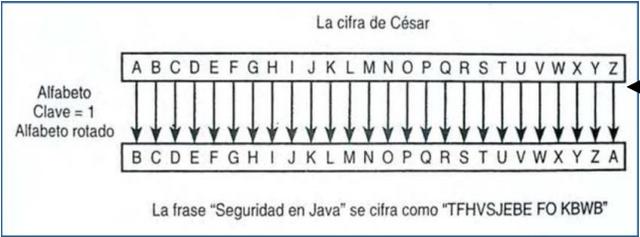


REDES DE COMPUTADORAS III

Lo esencial del cifrado es el concepto de algoritmos de cifrado y “claves”. Cuando se envía información, esta se cifra mediante un algoritmo y solo se puede descodificar con la clave apropiada. Una clave puede almacenarse en el sistema de recepción, o bien, transmitirse junto con los datos cifrados.



En criptografía, el cifrado César, también conocido como cifrado por desplazamiento, código de César o desplazamiento de César, es una de las técnicas de cifrado más simples y más usadas. Es un tipo de cifrado por sustitución en el que una letra en el texto original es reemplazada por otra letra que se encuentra un número fijo de posiciones más adelante en el alfabeto.



En criptografía, RSA (Rivest, Shamir y Adleman) es un sistema criptográfico de clave pública desarrollado en 1979. Es el primer y más utilizado algoritmo de este tipo y es válido tanto para cifrar como para firmar digitalmente. La seguridad de este algoritmo radica en el problema de la factorización de números enteros.



Data Encryption Standard (DES) es un algoritmo de cifrado, es decir, un método para cifrar información, El algoritmo fue controvertido al principio, con algunos elementos de diseño clasificados, una longitud de clave relativamente corta.

El principal problema de las claves simétricas es que para compartir la clave hay que enviarla a través de la red sin cifrar, lo que supone un riesgo de que alguien pueda interceptarla. La gran ventaja de las llaves simétricas es su simplicidad por lo que alcanzan un alto grado de rendimiento.

Las claves asimétricas se utilizan para proteger las claves simétricas. También se pueden utilizar para el cifrado de datos limitado y para firmar digitalmente objetos de base de datos. Una clave asimétrica se compone de una clave privada y su correspondiente clave pública.

