Nombre del alumno: Audelí Joachín Velázquez

Nombre del profesor: Lic. Lepe Arriaga Icel Bernardo

Nombre del trabajo: Cuadro sinóptico

Materia: Redes de computadoras III

Licenciatura: Ingeniería en sistemas computacionales

Grado: séptimo cuatrimestre

Grupo: “A”

Frontera Comalapa Chiapas a17 DE octubre de 2021

ALGORITMO DE CLAVE PUBLICA

ALGORITMO RSA

ESTA BASADO EN EL NOMBRE DE LOS INVENTORES: RIVEST, SHAMIR Y ADLEMAN ES UNA INTRODUCCION LAS BASES MATEMATICAS DICHO ALGORITMO DE ENCRIPTADO ESCRITO POR LLEGAR DESDE CONOCIMIENTO MINIMO

EL CONSEPTO DE ANILLO DE ENTERO, LA EXISTENCIA Y UNICIDAD DE LA DESCOMPOSICION EN FACTORES PRIMOS HASTA LA COMPRENCION DEL ALGORITMO EN SI PORLO QUE ES NECESARIO ESTUDIAR: ANILLO DE ENTERO MD, CONSEPTOS BASICOS DE LA ARITMETICA EN Z, MULTIPLOS Y DIVISORES, DIFINICIONES BASICAS, DESCOMPOSICION DE FACTORES PRIMOS , CALCULO DEL MCD Y DEL MCM POR DESCOMPOSICION.

OTROS DE ALGORITMO DE CLAVE PÚBLICA

SE BASA EN EL USO DE UNA PAREJA DE CLAVES PUBLICAS, PRIVADAS DE LAS CUALES UNA SE USA PARA CIFRAR Y LA OTRA PAR DECIFRAR POR LO QUE LA FUNCION SON IRREVERSIBLE A LA FUCION TRAMPA

OTRO PODEMOS VER QUE EN EL ALGORITMO DE DIFFIE-HELLMAN PUES ES UN PROTOCOLO PARA REALIZAR EL INTERCAMBIO DE CLAVES

FIRMA DE CLAVE SIMETRICA

LA CLAVE PRIVADA OFRECE UN METODO PAR EL DESARROLLO DE LA FIRMA DIGITAL PERMITIENDO AL RESEPTOR DE UN MENSAJE VERIFICAR LA AUTENTICIDAD DEL ORIGEN DE LA INFORMACION. LA DESVENTAJA ES QUE ES MUY LENTA

CUANDO SE ELABORABA EN MANUSCRITO ERA MAS FACIL PODER SABER SU CONTENIDO NO ASI CON LA FIRMA DIGITAL PORQUE SE TIENE QUE USAR UNA CLAVE PARA PODER SABER SU CONTENIDO

FIRMAS DE CLAVES PÚBLICA

SE VASA EN UNA FUNCION DE UN SOLO SENTIDO POR LO QUE VISTO DE OTRA FORMA EL COSTE COMPUTACIONAL REQUERIEDO ES MUY ALTO Y SU FUNCIONAMIENTO CRIPTOGRAFICO ES POR LA RSA.

LAS ADO UN UTORIDADES CERTIFICADAS SON PARA EL USO SEGURO LAS CLAVES PRIVADAS LA FN NT REALIZAN UNA FIRMA PROPIA Y SE INCLUYE LA EXPIRACION Y LA REVOACION

COMPRENDIOS DE MENSAJES

ES MUY IMPORTANTE LA LUY DE CONGRUENCIA, LA COMPATIBILIDAD DE LA REALACION CONGRUENCIA CON LA SUMA Y EL PRODUCTO.

SE NECECITA ANALIZAR LA ARITMETICA EN ZN PROPIEDADES Y LAS PROPORCIONES.

EL ATAQUE DE CUMPLEAÑOS

EXISTE UN ALT PROVABILIDAD QUE LA CLAVE QUE SE LE DA A NUESTRO ACCESO PUEDE SER LA DE NUESTRA FECHA DE NACIMIENTO

SEGÚN ARTICULOS TECNICOS COMO EL ALGORITMO DE HAS COMO SHA-10 MOS CUESTIONAN SU ROBUSTES Y ESTE VA DESARROLLADO GRACIAS AL AVANCE DE LAS MATEMATICAS