

prototipo_no_funcional2

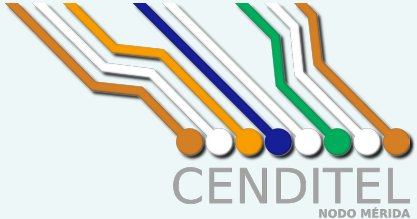
Exported at: Mon May 09 2016 08:56:18 GMT-0400 (BOT)

Inicio Bienvenida

Criptosistemas

Bienvenido


Criptosistemas



Generar Claves

Cifrar

Descifrar

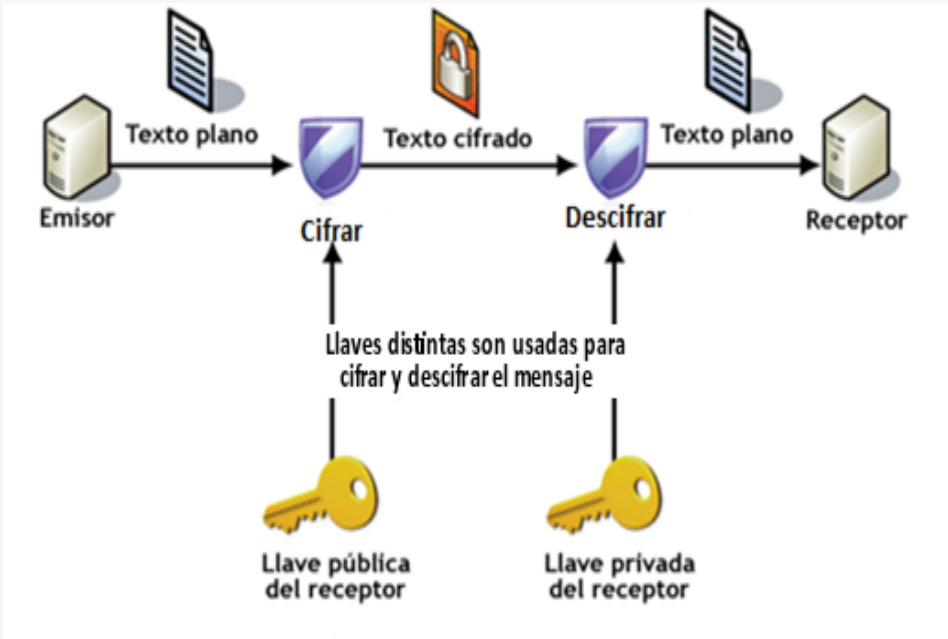


Seleccione Algoritmo

Criptosistema de Variedad Algebraica (CVA)

RSA

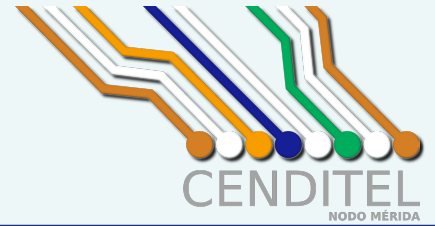
Elgamal



The diagram illustrates the asymmetric encryption process. It shows a flow from an **Emisor** (Sender) to a **Receptor** (Receiver). The process starts with **Texto plano** (Plain text) being sent to a **Cifrar** (Encrypt) step. This step uses a **Llave pública del receptor** (Receiver's public key). The result is **Texto cifrado** (Ciphertext), which is then sent to a **Descifrar** (Decrypt) step. This step uses a **Llave privada del receptor** (Receiver's private key). The final output is **Texto plano** (Plain text) received by the **Receptor**. A central text box states: "Llaves distintas son usadas para cifrar y descifrar el mensaje" (Different keys are used to encrypt and decrypt the message).

Bienvenido

Criptosistemas



Generar Claves

Cifrar

Descifrar



UNA DE LAS HERRAMIENTAS PRINCIPALES PARA PROVEER SEGURIDAD A LA INFORMACIÓN CUANDO SE TRANSMITE POR UN CANAL ABIERTO ES **LA CRIPTOGRAFÍA**. LA CRIPTOGRAFÍA ES UNA RAMA DE LA MATEMÁTICA QUE PERMITE TRANSFORMAR LA INFORMACIÓN DE MANERA QUE SU LECTURA SEA MUY DIFÍCIL SI NO SE POSEE UNA CLAVE CRIPTOGRÁFICA. ES DE PARTICULAR INTERÉS, ENTONCES, PARA ESTE CENTRO DE DESARROLLO E INVESTIGACIÓN EN TECNOLOGÍAS LIBRES-CENDITEL, DEDICAR PARTE DE SU POTENCIAL INVESTIGATIVO A ESTUDIAR LOS DIFERENTES SISTEMAS CRIPTOGRÁFICOS (CRIPTOSISTEMAS) EXISTENTES, PROPONER MEJORAS A LOS MISMOS O, INCLUSO, DESARROLLAR SOBERANAMENTE PROPUESTAS ALTERNATIVAS A LOS YA CONOCIDOS.

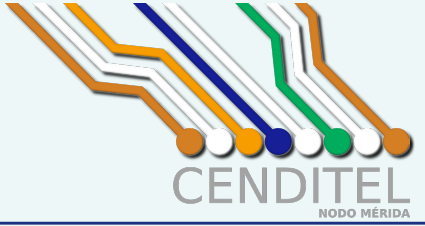
ES POR ELLO QUE DESDE CENDITEL NOS HEMOS PROPUESTO EL ESTUDIO DE UN CRIPTOSISTEMA NOVEDOSO QUE PUEDE DAR SEGURIDAD INCLUSO EN UN **COMPUTADOR CUÁNTICO**, SI LLEGARE A SER CONSTRUIDO. ESTE ESTUDIO SE LLAMA CRIPTOSISTEMA DE VARIEDAD ALGEBRAICA, SU SEGURIDAD SE BASA EN UN PROBLEMA MATEMÁTICO DEL ÁREA DE GEOMETRÍA ALGEBRAICA Y POSEE UNA COMPLEJIDAD COMPUTACIONAL **NP-COMPLETO**, LO CUAL LE PERMITIRÍA SER SEGURO EN EL MENCIONADO COMPUTADOR CUÁNTICO ADEMÁS DE PODER SER UTILIZADO EN UN COMPUTADOR CLÁSICO.

Boton "Generar Claves" (Evento Activo)

Criptosistemas

Generar Claves


Criptosistemas



Generar Claves


Cifrar

Descifrar



¿Deseas Generar las claves privada y publica?

Si



NO

Boton Si "Generar Claves" (Evento activo)

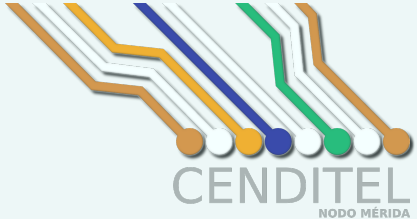


Boton "Cifrar" (Evento Activ)

Criptosistemas

Cifrar archivo


Criptosistemas



Generar Claves

Cifrar

Descifrar



Seleccionar Clave publica del usuario

PubKey Ana

PubKey Jose


PubKey Leo

PubKey Sulbaran

Seleccionar Archivo

nombre_archivo.txt

*Alerta tamaño maximo de archivo es de 256 Kb



Descargar en...

Se esta cifrando el archivo, espere ...

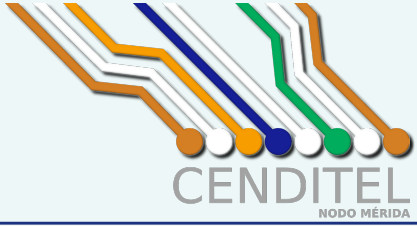
Se ha cifrado el archivo con Éxito ...

Boton "Descifrar" (Evento Activo)

Criptosistemas

Descifrar archivo


Criptosistemas



Generar Claves


Cifrar

Descifrar



Seleccionar Archivo

nombre_archivo_encryptado



Descifrar en...

Se esta descifrando el archivo, espere ...

Se ha descifrado el archivo con Éxito ...