SESION 6 1ER PARCIAL

Objetivo: al finalizar la sesión el alumno identificara los elementos y componentes del algoritmo de cifrado IDEA para encriptación y generación de llaves

Consideraciones teóricas:

Rivest, Shamir y Adlman son los creadores del algoritmo RSA que factoriza números muy grandes a partir de divisiones sucesivas Sus aplicaciones principales para la administración de la seguridad informática son:

Encriptación

Desencriptación

Generación de llaves publicas (para diversos usuarios) y llaves privadas (de forma especial uno o varios usuarios selectos)

Firmado digital

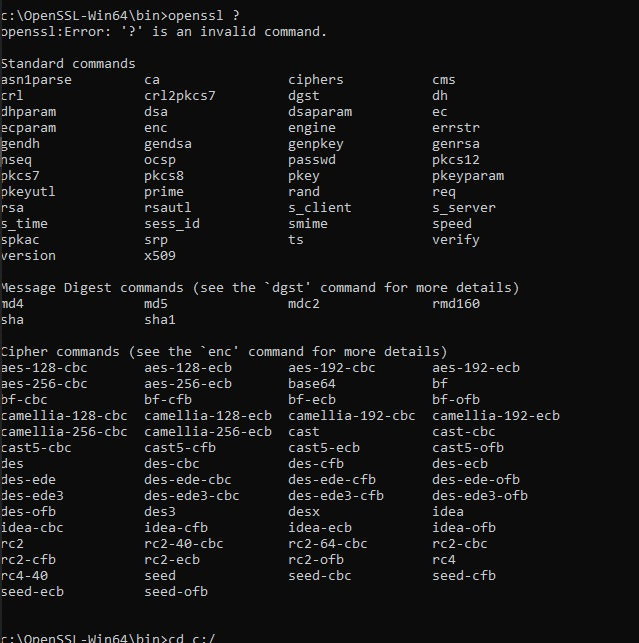
Certificados digitales

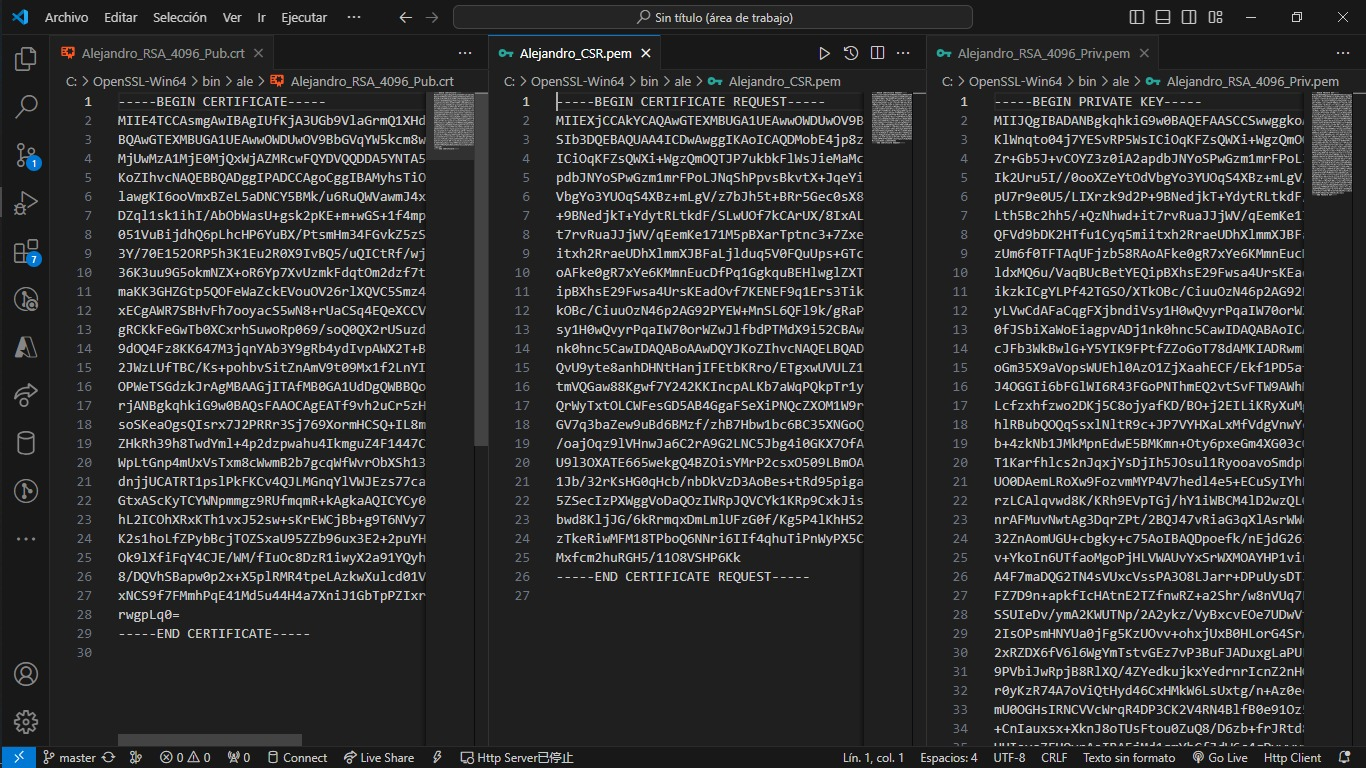
Su base es binaria por lo cal se puede tener en paridad de bits

256, 512, 1024, 2048, 4096 y mayores

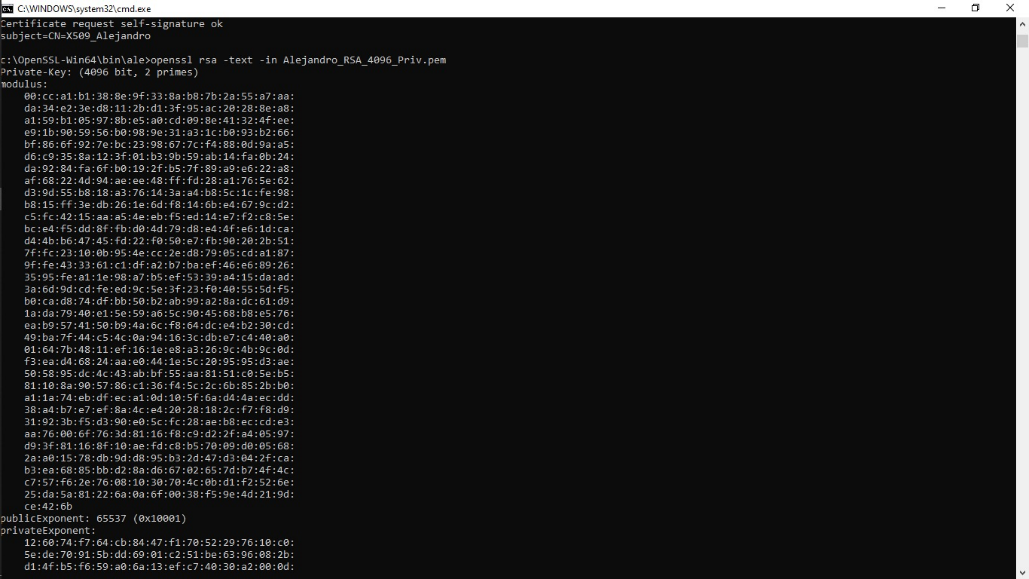
Desarrollo. Descargue Openssl para la generación de llaves RSA genere una de tipo publica y privada de 1024 bits, 2048 bits, 8192 bits

Definición de openSSL. Herramienta de código abierto que contiene un conjunto de funciones para la criptografía, toolkit para claves de cifrado RSA, firmas DSA, creación de certificados para páginas web x509, CRS, CRL SSL segurity socket layer y tls transport layer segurity

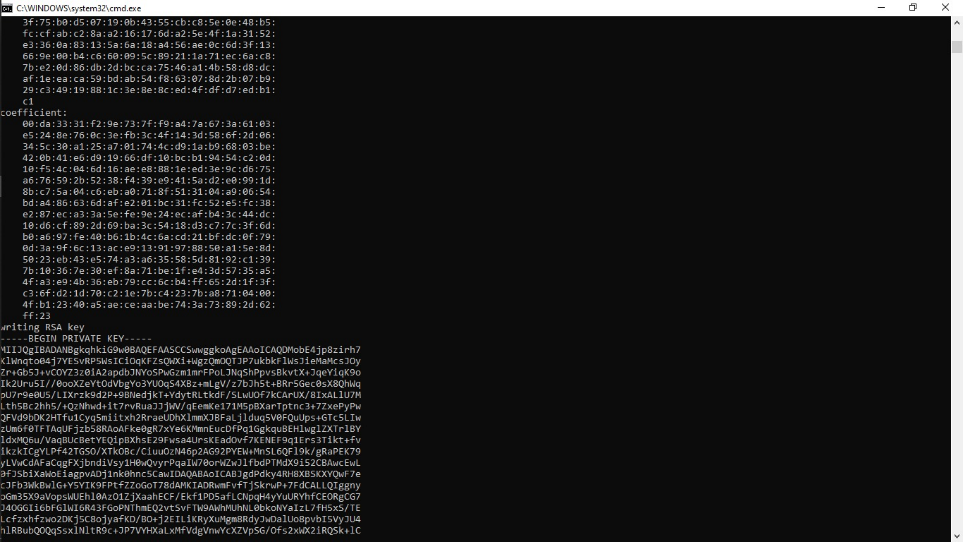




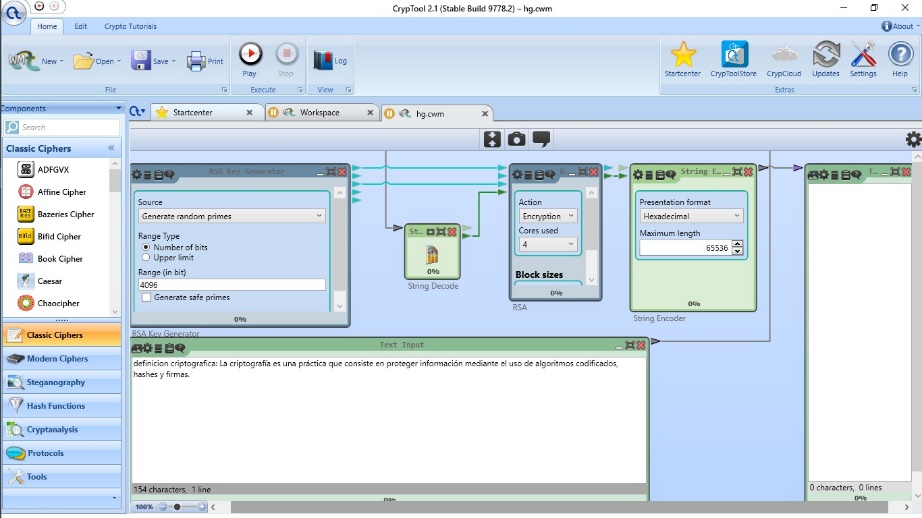
Desarrollo 1. Genere 2 llaves RSA de tipo publica y virtualice su estructura



Desarrollo 2. Genere 2 llaves RSA de tipo publicas y virtualice su estructura



Desarrollo 4 en la herramienta cryptool cifre la definición de criptografía, identifique todos sus componentes



En conclusión, RSA, OpenSSL y CryptoTools son herramientas fundamentales para asegurar la seguridad de los datos en el entorno digital. Su uso adecuado es crucial para proteger la información sensible de manera efectiva.