Protocolos Seguros con criptografía asimétrica y firmas digitales.

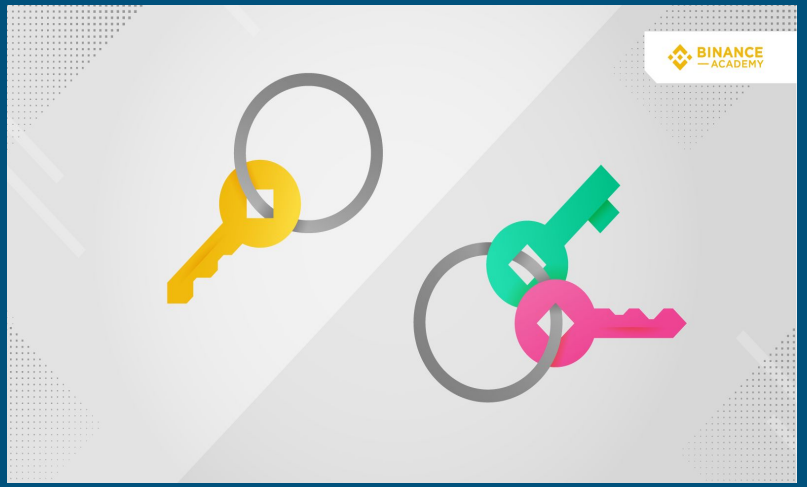
Integrantes:

-Contreras Mejía David
-López Castillón Jonathan Jhosua.
-Sánchez Pérez Omar Alejandro

Criptografía Grupo 1

Criptografía asimétrica

En este sistema, la clave pública se comparte libremente con otras personas, mientras que la clave privada se mantiene en secreto y solo la conoce su propietario. La clave pública se utiliza para cifrar los datos, mientras que la clave privada se utiliza para descifrarlos. La criptografía asimétrica proporciona un método seguro para intercambiar información sin necesidad de compartir claves secretas.



Firma digital

Es como un sello de seguridad que garantiza la autenticidad e integridad de un mensaje o documento. Es una forma de verificar que el remitente es quien dice ser y que el contenido del mensaje no ha sido alterado en el proceso de envío.

Proporciona seguridad y confianza en las comunicaciones electrónicas.

Implementación en Java

Para realizar la implementación se utilizaron dos clases, una para crear la firma digital y la otra para la verificación.

- GeneraFirma.java
- VerificaFirma.java

Secure Socket Layer (SSL)

Un certificado SSL es un protocolo de seguridad que autentica la identidad de un sitio web y habilita una conexión cifrada.

SSL utiliza el cifrado de clave pública y clave privada y otras funciones criptográficas para proteger las conexiones entre dispositivos que se comunican a través de una red TCP/IP.

TSL Transport Layer Security

Ha reemplazado gradualmente a SSL en la mayoría de las implementaciones. TLS presenta varias mejoras y actualizaciones en comparación con SSL.

Incluye protocolos y cifrados más seguros, y se actualiza periódicamente para abordar nuevas amenazas.

Referencias

Cifrado asimétrico. (s/f). IONOS Digital Guide. Recuperado el 14 de junio de 2023, de https://www.ionos.mx/digitalguide/servidores/seguridad/cifrado-asimetrico/

Firmas digitales y certificados. (s/f). Microsoft.com. Recuperado el 14 de junio de 2023, de https://support.microsoft.com/es-es/office/firmas-digitales-y-certificados-8186cd15-e7ac-4a16-8597-22bd163e8e96

IBM documentation. (2022, mayo 11). Ibm.com. https://www.ibm.com/docs/en/b2b-integrator/5.2?topic=522-secure-sockets-layers-ssl

TSL: qué significa este protocolo de seguridad I Sage Advice. (2020, mayo 20). Sage Advice España; Sage. https://www.sage.com/es-es/blog/diccionario-empresarial/tls/


Gracias