STUDIUL INDIVIDUAL NR. 1

Realizat de: Rija Dumitru

Grupa: W-2141

Profesor: Jeleascov Ioan

Disciplina: Project Management

Ceiti, 2024

Crearea Cheilor pentru Semnături Digitale (RSA și ECDSA)

Cuprins

Introducere în Semnăturile Digitale

Ce sunt semnăturile digitale?

Semnăturile digitale sunt o tehnologie care garantează:

1. Autenticitatea: Confirmă că un mesaj provine de la expeditorul intenționat.
2. Integritatea: Asigură că mesajul nu a fost modificat.
3. Non-repudierea: Expeditorul nu poate nega trimiterea mesajului.

Chei digitale:

Semnăturile digitale folosesc un sistem de chei:

- Cheie privată: Semnează documentele.
- Cheie publică: Verifică autenticitatea semnăturii.

Cheile RSA (Rivest–Shamir–Adleman)

CRIPTAREA

Ce este RSA?

Un algoritm criptografic folosit pentru semnături digitale și criptare.

Cum se generează cheile RSA?

- Cheia privată: Păstrată secretă și utilizată pentru a crea semnătura digitală.
- Cheia publică: Distribuită altora pentru a verifica semnătura.

Avantaje RSA:

- Ușor de implementat.
- Utilizat pe scară largă (ex.: HTTPS).
- Dezavantaje:
- Mai lent decât alte metode moderne.

- Necesită chei mari pentru securitate ridicată.

Cheile ECDSA (Elliptic Curve Digital Signature Algorithm)

Ce este ECDSA?

Un algoritm mai modern decât RSA, bazat pe matematică avansată (curbe eliptice).

Avantaje ECDSA:

- Eficient: consumă mai puține resurse.
- Rapid: potrivit pentru dispozitive mobile și criptomonede (ex.: Bitcoin).
- Dezavantaje:
- Mai complicat de implementat.

- Mai puțin utilizat în aplicații generale.

Cum se creează cheile pentru RSA și ECDSA?

1. **Alegerea unui algoritm:**

- RSA: dacă ai nevoie de compatibilitate largă.
- ECDSA: pentru eficiență și performanță.

2. **Generarea cheilor:**

- Utilizează librării sau software specializat:
- OpenSSL
- Alte unelte integrate în limbaje de programare (ex.: Python, Java).

3. **Stocarea cheilor:**

- Cheia privată: într-un loc securizat (ex.: manager de chei).
- Cheia publică: distribuită liber pentru verificare.

4. **Testare:**

- Semnează un document cu cheia privată și verifică semnătura cu cheia publică.

Rezumat pentru prezentare:

- RSA și ECDSA sunt două metode pentru generarea semnăturilor digitale.
- RSA este clasic, dar mai lent, în timp ce ECDSA este rapid și eficient.
- Cheile publice și private lucrează împreună pentru a asigura securitatea și integritatea datelor.

Bibliografie:

https://www.securitatea-informatiilor.ro/solutii-de-securitate-informatica/algoritmul-de-criptografie-rsa/

https://academy.binance.com/ro/articles/what-is-public-key-cryptography