Studiul Individual

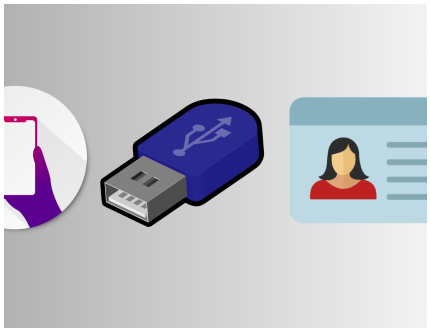
Elaborat de: Rija Dumitru, W-2141
Profesor: Jeleascov Ioan
Disciplina: Project Management

CEITI, 2024

Crearea Cheilor pentru Semnături Digitale (RSA și ECDSA)

Introducere

Semnătura digitală este un mecanism crucial pentru securitatea informației, asigurând integritatea și autenticitatea datelor. Algoritmii RSA și ECDSA sunt două metode de criptare utilizate frecvent pentru generarea și utilizarea cheilor în semnăturile digitale. Acest studiu explorează conceptele de bază, diferențele și aplicabilitatea lor.



Ce este o semnătura digitală?

Semnătura digitală este echivalentul electronic al unei semnături olografe. Prin intermediul acesteia, se poate confirma că:

1. Autenticitatea: Documentul provine de la expeditorul declarat.
2. Integritatea: Documentul nu a fost modificat după semnare.
3. Non-repudierea: Expeditorul nu poate nega că a semnat documentul.

Pentru a implementa semnătura digitală, sunt utilizate algoritmi criptografici care implică un sistem de chei publice și chei private.

Algoritmi populari pentru semnături digitale

1. RSA (Rivest-Shamir-Adleman)

RSA este unul dintre cei mai vechi și răspândiți algoritmi criptografici. Acesta se bazează pe dificultatea factorizării numerelor mari.

Procesul de generare a cheilor RSA:

- Cheia publică (e, n): Utilizată pentru verificare.
- Cheia privată (d, n): Utilizată pentru semnare.
- Formula matematică:
- Generăm două numere prime mari p și q.
- Calculăm $n = p \times q$.
- Determinăm $\phi(n) = (p - 1) \times (q - 1)$.
- Alegem un e, unde $1 < e < \phi(n)$, astfel încât e și $\phi(n)$ să fie prime între ele.
- Calculăm d, inversul modular al lui e mod $\phi(n)$.

Avantaje:

- Simplitatea implementării.
- Aplicații largi în semnături și criptare.

Dezavantaje:

- Chei mari necesare pentru o securitate ridicată (2048 sau 4096 biți).
- Lent pentru dispozitive cu resurse limitate.

ECDSA (Elliptic Curve Digital Signature Algorithm)

ECDSA este un algoritm mai modern care folosește matematica curbelor eliptice pentru semnături digitale. Este o alternativă mai eficientă decât RSA, mai ales în medii restrânse.

Procesul de generare a cheilor ECDSA:

- Alegem o curbă eliptică definită de ecuația $y^2 = x^3 + ax + b$ peste un câmp finit.
- Generăm un punct generator G pe această curbă.
- Cheia privată (d): Un număr aleator ales în intervalul [1, n-1], unde n este ordinea lui G.
- Cheia publică (Q): $Q = d \times G$.

Avantaje:

- Dimensiuni reduse ale cheilor (256 biți pentru securitate echivalentă cu RSA 3072).
- Performanță ridicată pe dispozitive mobile.

Dezavantaje:

- Implementare mai complexă.
- Necesită mai multă expertiză pentru configurare corectă.

Diferențe RSA vs. ECDSA

Caracteristică	RSA	ECDSA
Metodă matematică	Factorizare de numere mari	Curbe eliptice
Dimensiune cheie	Mare (2048-4096 biți)	Mică (256-512 biți)
Viteză	Mai lent	Mai rapid
Aplicații	Certificate SSL, criptare	Criptomonede, IoT

Exemple de utilizare

1. Semnături în blockchain: Bitcoin și alte criptomonede utilizează ECDSA pentru tranzacții sigure.
2. Certificat SSL/TLS: RSA este folosit pentru securizarea conexiunilor web.
3. IoT (Internet of Things): ECDSA este preferat datorită eficienței sale.

Concluzie

RSA și ECDSA sunt algoritmi esențiali pentru semnăturile digitale. RSA oferă o soluție matură, dar depășită în unele aplicații moderne, în timp ce ECDSA este mai eficient și mai sigur pentru dispozitivele moderne. Alegerea între acești algoritmi depinde de cerințele de securitate, resursele disponibile și specificul aplicației.

Bibliografie

1. https://academy.binance.com/ro/articles/what-is-public-key-cryptography
2. https://stisc.gov.md/ro/semnatura-electronica
3. https://www.scribd.com/document/605373552/Securitatea-Spatiului-Cibernetic-Laboratorul-5