Prezentare Proiect – Autentificare prin Semnătură Digitală

# 1. Scopul Proiectului

Proiectul demonstrează o metodă modernă de autentificare bazată pe semnătură digitală, utilizând algoritmi de criptografie cu cheie publică (ECDSA) și funcții hash (SHA-256). Sistemul permite generarea de chei, semnarea de fișiere, verificarea semnăturii și autentificarea utilizatorului fără parolă.

# 2. Funcționalități Implementate

- Generare pereche de chei (privată/publică) folosind ECDSA

- Criptare cheie privată cu parolă și salvare în siguranță

- Semnarea digitală a fișierelor selectate de utilizator

- Verificarea semnăturii cu cheia publică

- Autentificare pe bază de semnătură: semnare challenge (nonce) și validare identitate

# 3. Tehnologii Folosite

- Python 3

- Tkinter pentru GUI

- ecdsa pentru semnături digitale

- cryptography pentru criptare cu parolă

- hashlib pentru generarea hash-ului (SHA-256)

# 4. Justificare Tehnică

Sistemele clasice de autentificare se bazează pe parole, care pot fi ghicite sau furate. Această aplicație înlocuiește parola cu semnătura digitală, semnând un mesaj aleator (nonce). Doar posesorul cheii private poate genera o semnătură validă, ceea ce asigură autentificare sigură, fără transmiterea de secrete.

# 5. Fluxul Aplicației

1. Utilizatorul generează o pereche de chei și își protejează cheia privată cu o parolă.

2. Aplicația poate semna orice fișier și salva semnătura digitală separată.

3. Oricine poate verifica autenticitatea unui fișier cu semnătura și cheia publică.

4. Pentru autentificare, aplicația generează un challenge și îl semnează; validarea se face cu cheia publică.

# 6. Valoare Practică

Proiectul simulează un sistem real de autentificare utilizat în aplicații precum: e-guvernare, banking digital, blockchain, semnare contracte electronice. Demonstrează aplicarea directă a criptografiei în securitatea informatică.