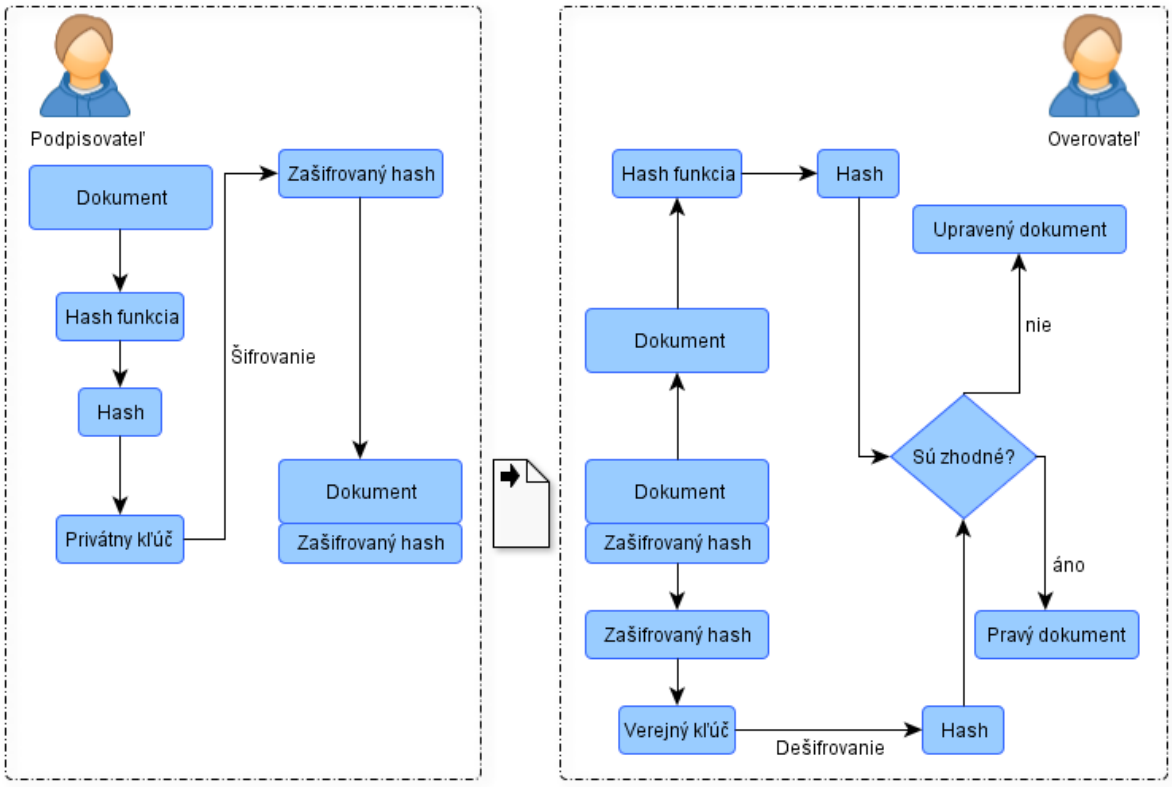
Zadání úlohy – Elektronický podpis

Váš závěrečný projekt je naprogramování aplikace, která budou sloužit k elektronickému podepsáni souboru. Princip je znázorněn na obrázku níže (pokud nerozumíte slověnštině, viz info tabule na cvičení :)):

Vaším záverečným projektem bude naprogramovat aplikaci na práci s elektronickým podpisem. Princip elektronického podpisu je znázorněný na obrázku:



Hashovací funkce SHA-256 umožňuje podepsat prakticky jakýkoliv soubor (načítejte pomocí "rb") a o skoro libovolné velikosti.

Řešení bude obsahovat:

- Načtení souborů pro podpis (fileDialog)
- Zobrazení podrobností o podepisovaném souboru -> Název, cesta, typ (přípona), velikost, datum úpravy apod.
- Podepsání souboru pomocí funkcí RSA a SHA256. (Je nutné využít RSA, které jste implementovali v předchozí úloze)
- Ověření podpisu
- Generování klíčového páru s exportem do souborů (.priv a .pub)
- Uživatelské rozhraní - kompletně interaktivní (volba souboru v dialogovém okně - hodně vašich kolegů to zná (fileDialog)), tlačítka, v podstatě není potřeba vstupních polí na text.

Doplňující informace:

- Elektronický podpis (výstup po hashování a po zašifrování pomocí RSA -> soubor s příponou .sign). Obsah souboru bude vypadat následovně:

  RSA_SHA256 PODPIS_V_BASE64. (například "RSA_SHA256 QWhvaiBQZXBvLCBqYWsgc2UgbcOhxaEgPw==")

- Soubor .sign bude spolu s podepisovaným dokumentem zabalem do souboru .zip a exportovaný uživatelem, tam kam chce (fileDialog).
- Klíčový pár budou dva soubory s připonou .priv (soukromý) a .pub (veřejný) a obsah bude ve tvaru:

  RSA SOUKROMÝ_KLÍČ_V_BASE64.
  RSA VEŘEJNÝ_KLÍČ_V_BASE64.

- Ověřování by mělo probíhat při volbě veřejného klíče a souboru .zip (bez nutnosti hledat a ručně rozbalovat podpis).

Bodové ohodnocení:

1. Načtení souboru pro podepsání a zobrazení základních informací (název, cesta, datum vytvoření, typ, apod.) - 2 body
2. Vygenerování klíčů a podepsání souboru pomocí SHA-256 a RSA - 4 body
3. Ověření dokumentu na základě elektronického podpisu - 4 body
4. Manipulace se soubory s klíčí a el. podpisem (načítání a ukládání souborů s příponami priv, .pub a .sign (.zip)) - 4 bodů
5. GUI (plně interaktivní s tlačítky pro načítání/ukládání souborů, zobrazení potřebných informací) - 4 bodů
6. Umělecký dojem – 2 body

Bonusové body za kreativitu.