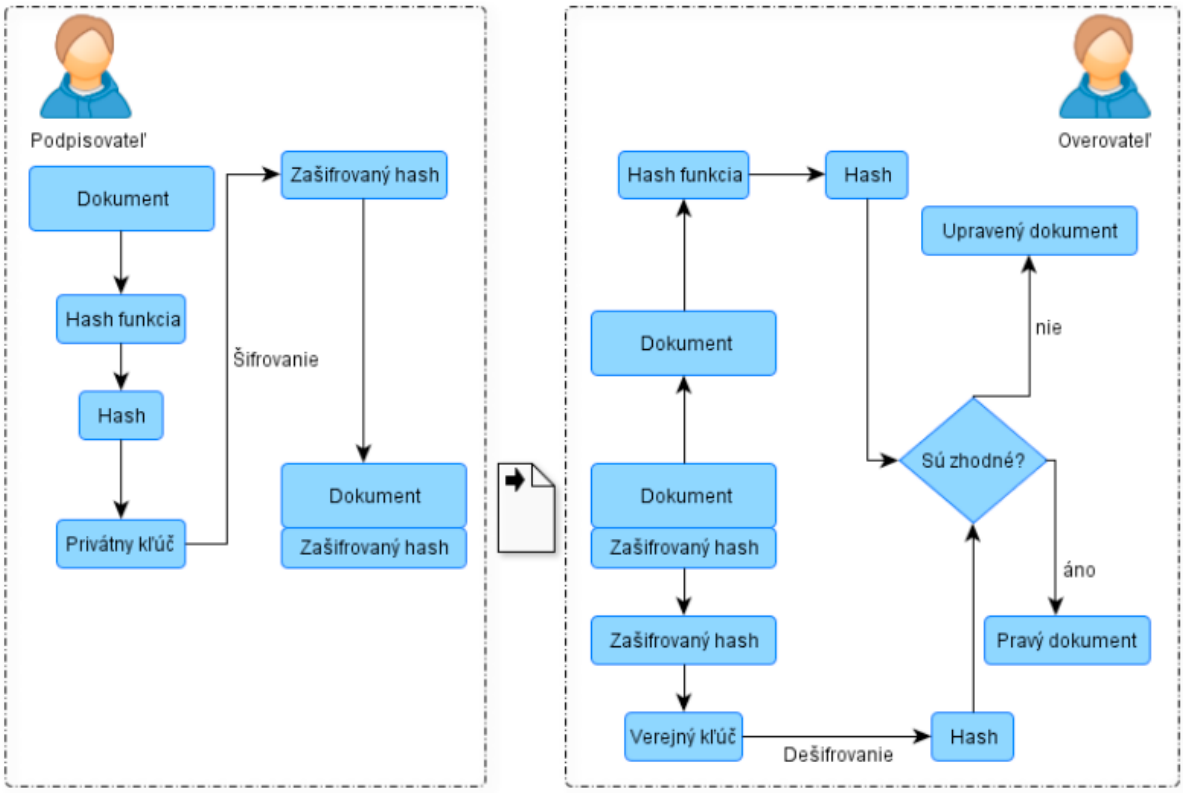
Zadání úlohy – Elektronický podpis

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

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



Hashovací funkce SHA3-512 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 SHA3-512 Keccak. (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_SHA3-512 PODPIS_V_BASE64. (například "RSA_SHA3-512 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).

!!! BODY jsou pouze ORIENTAČNÍ !!! PLATÍ HODNOCENÍ PROŠEL / NEPROŠEL !!!

Celkově je možno získat 10 bodů. 6 je potřeba a bude hodnoceno známkou „Prošel“

Bodové ohodnocení:
1. Načtení souboru pro podepsání a zobrazení základních informací (název, cesta, datum vytvoření, typ, apod.) - 1 bod

2. Vygenerování klíčů a podepsání souboru pomocí SHA3-512 a RSA - 2 body

3. Ověření dokumentu na základě elektronického podpisu - 2 body

4. Manipulace se soubory s klíčí a el. podpisem (načítání a ukládání souborů s příponami priv, .pub a .sign (.zip)) - 2 bodů

5. GUI (plně interaktivní s tlačítky pro načítání/ukládání souborů, zobrazení potřebných informací) - 2 bodů

6. Umělecký dojem – 1 bod

Bonusové body za kreativitu.

Tento úkol odevzdejte 14 dní od zadání na cvičení. (viz podmínky k zápočtu a deadline v MOODLE)
Máte na vypracování čas 14 dní, tj do přespříštího cvičení. Je to tak schválně, abyste během příštího cvičení mohli konzultovat s vyučujícím případné problémy, co se týče naprogramování úkolu. V případě dotazů se ptejte.