Generátor úloh do aplikované kryptografie
Kontrolní studie

Michal Homola,
Dominik Chrenčík,
Jiří Marák,
Vojtěch Lukáš

21. dubna 2023

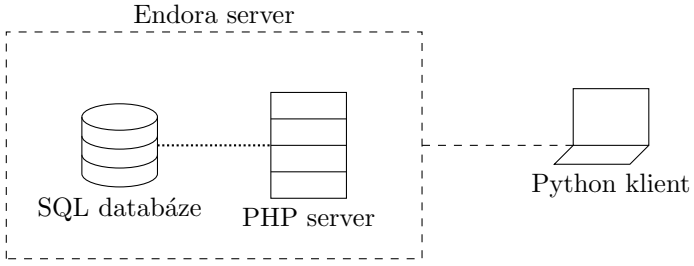
Obsah

Úvod

Předmětem této dokumentace je představit vizi projektu s názvem „Generátor kryptografických úloh“. První část bude věnována teoretickému popisu systému jako celku. ...

1 Architektura

Schéma systému lze vidět na obr. 1. Úlohy jsou uloženy v SQL databázi. K této databázi má přístup pouze webový PHP server. Ten slouží jako „prostředník“ mezi klientem a databází. Dále do úloh vkládá generované hodnoty (klíče apod.). Klientská aplikace funguje jako přístupový bod a sehrává roli prezentační vrstvy. Pro jednoduchost je vyvinuta v jazyce Python, využívá pouze konzolové prostředí.



Obrázek 1: Schéma systému

1.1 Konstrukce databáze

V tabulce 1 lze vidět strukturu SQL databáze. Sloupec **ID** slouží jako primární klíč databáze, **Kód** úlohy pak slouží pro snazší rozlišení úloh. V buňce **Zadání** se nachází textový popis úlohy. Zde stojí za povšimnutí, že všechny číselné hodnoty důležité k výpočtu jsou nahrazeny zástupnými znaky „$\$n$“. Na místa těchto znaků bude logika v back-endu vkládat vygenerované hodnoty. Díky tomu bude možno jednu úlohu řešit vícekrát, pokaždé s jinými parametry. Pole **Výsledek** je záměrně prázdné – správný výsledek zde vloží až server, který tuto hodnotu vypočítá podle vygenerovaných parametrů.

Tabulka 1: Struktura SQL databáze

ID `INT`	**Kód** `VARCHAR(5)`	**Zadání** `TEXT`	**Nápověda** `TEXT`	**Výsledek** `TEXT`
1	`PR`	Rozhodněte (ano/ne) zda je číslo $n = \$1$ prvočíslo	...	`NULL`
2	`RSAe`	Zašifrujte zprávu $m = \$4$, pomocí RSA kryptosystému. Prvočísla jsou $p = \$1$; $q = \$2$, a soukromý klíč je $e = \$3$	...	`NULL`
⋮	⋮	⋮	⋮	⋮

Uživatel si bude moct vybrat jaký typ bude chtít řešit, back-end si tuto úlohu podle jejího kódu vytáhne z databáze, opatří ji vygenerovanými operandy a spolu se správným výsledkem a nápovědou ji zašle uživateli, jak lze vidět v diagramu na obr. TODO::diagram!