Generátor úloh do aplikované kryptografie

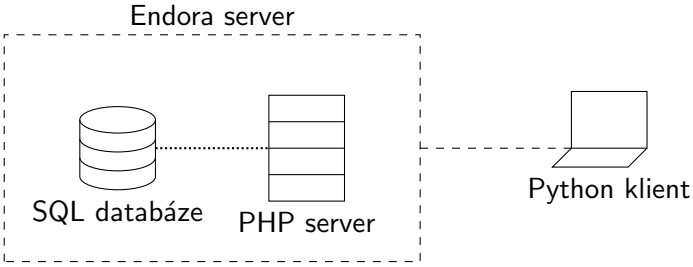
Michal Homola, Dominik Chrenčík, Jiří Marák, Vojtěch Lukáš

MPC-KRY
Ústav telekomunikací
VUT v Brně

26. dubna 2023

Zadání

Navrhněte a implementujte vlastní službu pro generování úloh do aplikované kryptografie. Služba bude mít vlastní rozhraní **(REST API)**, prostřednictvím kterého bude možné vyžádat úlohu **(HTTP metoda GET)**. Úloha se bude předávat ve formátu **JSON**. Úlohy se budou generovat **do konzole**.



Obrázek: Schéma vyvinutého systému

- databáze je navržena pro maximalizaci variability
- prototypy úloh, do kterých jsou na serveru dosazeny náhodné hodnoty
- token $\$n$
- pole **result** je prázdné, výsledek je dosazen až po generaci hodnot

Tabulka: Struktura databáze

code	**description**	**result**	**hint**
dh	Vypočítejte soukromý klíč pomocí DH. Prvočíslo $p = \$1 \ldots$	NULL	Nápověda...
lcm	Najděte nejmenší společný násobek čísel \$1 a \$2.	NULL	Nápověda...
⋮	⋮	⋮	⋮

Generátor hodnot

- součást back-end serveru, logika implementována v PHP
- hodnoty jsou generovány náhodně, následně je kontrolvána jejich správnost
- z hodnot je vypočítán výsledek – obojí následně předáno další vrstvě

ukázka kódu

```
$random = rand(1,2); //slouzi k vyberu prvocislo / slozene cislo
                     //podle vyberu se operand $prime nastavi na True/False
if ($random == 1) {
//prvocislo
$X = rand(530, 10000);
$C = gmp\_nextprime($X); //vysledek
$prime= True;
} else {
//slozene cislo
}

```

Back-end server

- vyvinut v PHP: `<url> = http://vut-fekt-mpckry-gr14.8u.cz/index.php`
- implementuje REST

Tabulka: API funkce serveru

URL	popis	použití
`/alltasks`	zašle všechny úlohy z DB	`<url>/alltasks`
`/task?code=<code>`	zašle úlohu s daným kódem	`<url>/task?code=dh`
`/randomtask`	zašle náhodnou úlohu	`<url>/randomtask`

Front-end klient

- vyvinut jako skript v Pythonu
- žádá back-end GET requestem, přijímá JSON objekty, které následně zobrazí

- DEMO

Příklad kódu

Příklad Python kódu

```python

while True:
    valid_codes = print_all_tasks()
    code = str(input(f"{C_BLUE}[Skore: {SCORE}] {C_YELLOW}Zadejte kod ulohy, kterou si prejete resit:{C_RES}"))
    if code not in valid_codes:
        print(f"{C_RED}spatny kod{C_RES}")
    else:
        clear_console()
        request = requests.get(f"{API}/task?code={code}")
```

Příklad PHP kódu

```php
$random = rand(1,2); //slouzi k vyberu prvocislo / slozene cislo
//podle vyberu se operand $prime nastavi na True/False
if ($random == 1) {
//prvocislo
$X = rand(530, 10000);
$C = gmp_nextprime($X); //vysledek

$prime= True;

} else {
//slozene cislo
```

Dosažené výsledky

- Funkční generátor