Generátor úloh do aplikované kryptografie

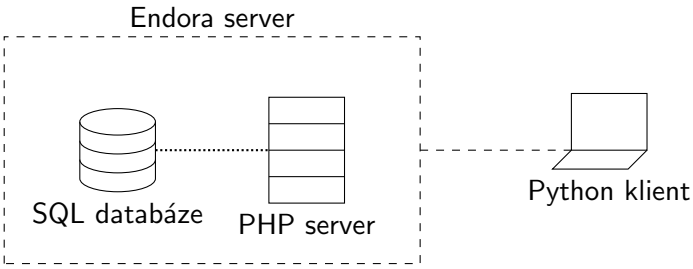
Michal Homola, Dominik Chrenčík, Jiří Marák, Vojtěch Lukáš

MPC-KRY
Ústav telekomunikací
VUT v Brně

20. 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

Back-end server

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

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`

Unordered lists

- Lorem ipsum dolor sit amet, consectetuer adipiscing elit.
- Etiam sapien elit, consequat eget, tristique non, venenatis quis, ante.
- Aliquam erat volutpat.
- Integer lacinia.
- Cras pede libero, dapibus nec, pretium sit amet, tempor quis.

Ordered lists

1. Lorem ipsum dolor sit amet, consectetuer adipiscing elit.
2. Etiam sapien elit, consequat eget, tristique non, venenatis quis, ante.
3. Aliquam erat volutpat:
   - Integer lacinia.
   - Cras pede libero, dapibus nec, pretium sit amet, tempor quis.

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam sapien elit, consequat eget, tristique non, venenatis quis, ante. Duis sapien nunc, commodo et, interdum suscipit, sollicitudin et, dolor.

`Fusce tellus.` Praesent in mauris eu tortor porttitor accumsan. Nullam feugiat, turpis at pulvinar vulputate, erat libero tristique tellus, nec bibendum odio risus sit amet ante. Vestibulum fermentum tortor id mi.

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam sapien elit, consequat eget, tristique non, venenatis quis, ante. Duis sapien nunc, commodo et, interdum suscipit, sollicitudin et, dolor.

Fusce tellus. Praesent in mauris eu tortor porttitor accumsan. Nullam feugiat, turpis at pulvinar vulputate, erat libero tristique tellus, nec bibendum odio risus sit amet ante. Vestibulum fermentum tortor id mi.

Obrázek: Your caption

Tabulka: Your caption

Function name	Duration	Complexity	Length	Score
Algo 1	0.0159	0.50	125	78
Algo 2	0.0453	0.65	854	88
Algo 3	0.8642	0.77	84	95
Algo 4	0.0020	0.24	638	76

Pythagorean theorem can be written in one short equation as: $a^2 + b^2 = c^2$ where c is the longest side of the triangle, a and b are the other two sides.

Other useful equations (thank you *John Napier*):

$$\log_b(x \cdot y) = \log_b(x) + \log_b(y) \tag{1}$$

$$\log_b\left(\frac{x}{y}\right) = \log_b(x) - \log_b(y) \tag{2}$$

$$\log_b(x^p) = p \cdot \log_b(x) \tag{3}$$

$$\log_b(x) = y \quad \text{exactly if} \quad b^y = x \tag{4}$$

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