

# Generátor úloh do aplikované kryptografie

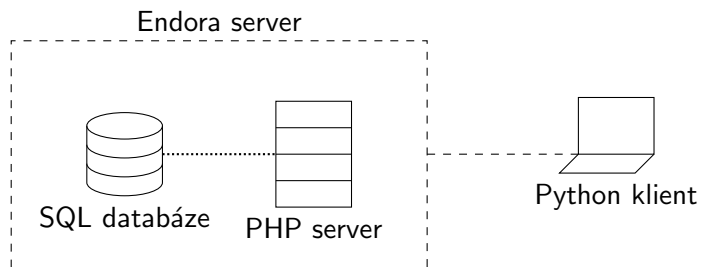
Michal Homola, Dominik Chrenčík, Jiří Marák, Vojtěch Lukáš

MPC-KRY  
Ústav telekomunikací  
VUT v Brně

26. dubna 2023



Navrhňte 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 $p = \$1 \dots$	NULL	Nápověda...
lcm	Najděte nejmenší společný násobek čísel $\$1$ a $\$2$ .	NULL	Nápověda...
$\vdots$	$\vdots$	$\vdots$	$\vdots$

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

## ukázka kódu

```
1 $random = rand(1,2); //slouzi k vyberu prvocislo / slozene cislo
2                               //podle vyberu se operand $prime nastavi na True/False
3 if ($random == 1) {
4 //prvocislo
5 $X = rand(530, 10000);
6 $C = gmp\_nextprime($X); //vysledek
7 $prime= True;
8 } else {
9 //slozene cislo
10 }
11
```

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

Tabulka: API funkce serveru

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

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

Q&A

Děkujeme za pozornost!