

## System ankietowy — szyfrowanie po stronie klienta



Ankiety hostowane statycznie (GitHub Pages). Odpowiedzi szyfrowane w przeglądarce (RSA-OAEP + AES-GCM) i wysyłane na lekki serwer Python + aiohttp + SQLite3.

[Ankieta](#)[Panel analityka](#)[Przeglądarka kodu projektu](#)

### O projekcie

Projekt powstał, by ułatwić zespołom badawczym szybkie uruchomienie bezpiecznych ankiet bez potrzeby konfigurowania skomplikowanej infrastruktury. Statyczna strona (np. GitHub Pages) działa jako frontend — to tam generujemy klucze, szyfrujemy odpowiedzi po stronie klienta i wysyłamy do prostego API serwera zapisu.

### Główne założenia

#### ● Bezpieczeństwo

Szyfrowanie end-to-end: RSA-OAEP (dla klucza sesji) + AES-GCM (dla treści odpowiedzi). Tylko analityk z tokenem może odszyfrować dane.

#### ● Lekki backend

Python + aiohttp + SQLite3 — minimum zależności, łatwe uruchomienie na tanim VPS (mikrokontenery, kopiowanie konfiguracji).

#### ● Rola analityka

Osoba z dostępem (token 16 znaków) może pobierać zaszyfrowane rekordy, odszyfrować lokalnie i uruchomić wstępne przetwarzanie/analizy.

### Skąd pomysł?

Projekt powstał w wyniku współpracy z młodymi zespołami badawczymi na Uniwersytecie Rzeszowskim — często brakowało im prostych rozwiązań IT. Chciałem dać narzędzie, które działa "out of the box": statyczny frontend, proste API i bezpieczny pipeline danych.

**Notka techniczna:** W systemie frontend generuje klucz sesji (AES-GCM), szyfruje odpowiedzi, a klucz sesji jest asymetrycznie szyfrowany RSA-OAEP przy użyciu publicznego klucza analityka. Serwer przechowuje jedynie zaszyfrowane paczki — odszyfrowanie i analiza odbywa się po stronie analityka.

### Panel analityka (demo)

Wprowadź token dostępu (16 znaków)

[Kopiuuj](#)

Token to jedyny sekret, który nadajesz analitykowi. W praktyce: token powinien być bezpiecznie przekazany — np. poza systemem (SMS, e-mail zaszyfrowany, itp.).

### Dlaczego to tanie i skalowalne?

Podejście "mikrusowania" — wystawiasz niewielką usługę (mały VPS / kontener). Skala = kopiuje + zmień token i port. Dzięki temu koszty utrzymania są niskie, a wdrożenie szybkie.

Lekkie   Skalowalne   Bezpieczne (E2E)

### Badania kliniczne — zaproszenie

Jeśli czytasz ten tekst i rozważasz udział w badaniu klinicznym testującym schemat działania cytyzyny (lek stosowany w terapii rzucania palenia) — warto zapoznać się z aktualnymi badaniami prowadzonymi m.in. w Uniwersytecie Rzeszowskim.

[Szczegóły badania UR](#)

Uczestnictwo w badaniach klinicznych to świadoma decyzja — zawsze zapoznaj się z kryteriami włączenia/wylączenia i formularzem świadomej zgody.

Przejdź do ankiety

Przejdź do  
Panelu Analityka

Zobacz kod  
projektu

Więcej informacji  
o badaniu z cytyzyną

## Ankieta: Wiedza o Uzależnieniu od Nikotyny

1. Jaka jest główna substancja uzależniająca w papierosach?

- ☐ Kofeina
- ☐ Nikotyna
- ☐ Tlenek węgla

2. Czy nikotyna jest substancją działającą krótko czy długo?

- ☐ Krótko (kilka godzin)
- ☐ Długo (cały dzień)

3. Najczęstszy objaw odstawienia nikotyny to:

- ☐ Nadmierna senność
- ☐ Wzrost apetytu i drażliwość
- ☐ Nagłe obniżenie ciśnienia

**Zaszyfruj i wyślij odpowiedź -**

**Wyślij i Zaszyfruj Odpowiedzi**

## Przeglądarka kodu projektu

## Zobacz kod wybranego pliku projektu -

info.txt

Kod zawiera przykład formatu odpowiedzi zwracanej przez stronę ankiety, oraz jej schematu

```
{ "Główna substancja uzależniająca": "'Nikotyna'", "Czas działania nikotyny": "'Krótko (kilka godzin)'", "Najczęstszy objaw odstawienia": "string" }
```

Niniejszy kod służy za część dokumentacji

[Przygotuj klucze](#)[Przetestuj klucze](#)[Zarządzaj danymi](#)**- Wybierz zakładkę**

## Tworzenie kluczy, tokenów i schematu danych

Unikalny Token (URL-safe Base64, 16 znaków)

Wprowadź token lub użyj generatora

**Generator tworzy bezpieczny token, choć możesz go wpisać ręcznie**[Generuj Token](#)

Wprowadź url serwera

np. `https://frog01-21435.wykr.as`

**Tu wpisz adres url serwera na który przesyłane są dane**

Schemat Danych (JSON)

Zdefiniuj strukturę danych. Użyj nazw pól (keys) identycznych jak w bazie danych, przypisując im typy (np. 'int', 'float', 'string', 'boolean').

```
{
  "record_id": "number",
  "device_name": "string",
  "is_active": "boolean"
}
```

**Schemat danych służy wykluczeniu danych o nieprawidłowej strukturze  
W celu zapobieżenia błędom wna etapie ich wstępnego przetwarzania**

Klucz Publiczny (JWK)

Tutaj pojawi się wygenerowany klucz publiczny w formacie JWK

**Ten kod kopiujesz do HTML strony z ankietą – wyjaśnienie na następnym slajdzie**

Klucz Prywatny (JWK)

Tutaj pojawi się wygenerowany klucz prywatny w formacie JWK

[Generuj Klucze \(JWK\)](#)**Tu generujesz 2 klucze RSA**[Eksportuj Dane \(JSON\)](#)**Tu pobierasz 2 pliku – jeden z kluczem publicznym, drugi z resztą danych**

```
const API_BASE_URL = 'https://frog01-21435.wykr.es';
```

**Tu wklejasz adres serwera z bazą danych**

```
// ** UWAGA: Wklej swój prawidłowy obiekt JWK poniżej  
// Aktualnie jest to pusty obiekt.
```

```
const JWK_PUB_KEY = `{
```

```
"alg": "RSA-OAEP-256",
```

```
"e": "AQAB",
```

```
"ext": true,
```

```
"key_ops": [
```

```
  "encrypt",
```

```
  "wrapKey"
```

```
],
```

```
"kty": "RSA",
```

```
"n": "rPZw1w1uHJ1VmePhLJwDAPTLZ6iQpfry3XDnH0_E_RC7oHf_1EnVk5
```

```
}`;
```

**Tu wklejasz tekst klucza publicznego**

```
DB_PATH = 'survey_data.db'
```

```
ACCESS_TOKEN = 'BardzoTajnyTokenDostepu123'
```

```
TABLE_NAME = 'surveys'
```

**W kodzie serwera ustaw ten sam token dostępu**

# Panel analityka danych

Przygotuj klucze

Przetestuj klucze

Zarządzaj danymi

## Testowanie kluczy

Załaduj klucze i dane analityczne, wprowadź przykładowe dane, a następnie przetestuj proces szyfrowania/deszyfrowania oraz walidacji schematu.

### Klucz Publiczny RSA-OAEP (JWK)

Nie wybrano pliku

**Tu ładujesz dwa pliki: ...public.json i ...analytic.json**

### Plik Danych Analitycznych (analytic.json)

Nie wybrano pliku

### Wprowadź Przykładowe Dane JSON do Szyfrowania

```
{"id": 123, "name": "Testowy Rekord", "isActive": true}
```

**Tu wpisujesz wiadomość do zakodowania w JSON zgodnym z schematem – z panelu „Przygotuj klucze”**

Testuj Szyfrowanie, Deszyfrowanie i Walidację (Oczekiwanie na klucze)

### Wynik Deszyfrowania i Walidacji

Odkodowana wiadomość pojawi się tutaj po udanym teście.

**Tu pojawi się odszyfrowana wiadomość – lub komunikat o błędzie + na jakim etapie wystąpił**

# Panel analityka danych

Przygotuj klucze

Przetestuj klucze

Zarządzaj danymi

## Zarządzanie Danymi

Wczytaj pliki JSON (wiele plików):

Wybierz pliki

Nie wybrano pliku

**Tu wczytujesz pliki JSON z kopiami zapasowymi bazy danych – program scala te dane**

☒ Użyj danych ze zmiennej globalnej (zamiast serwera)

**Jeśli zaznaczone program operuje na danych z wczytanych z plików – jeśli nie na danych z serwera**

Wyświetl Dane

Usuń Dane

Eksportuj Dane

**„Wyświetl Dane” na dole strony pojawia się tabela ze wszystkimi danymi – możesz ją skopiować np. do Excell**

Komunikat ze strony farma.1ioe.top

Czy na pewno chcesz usunąć zawartość bazy danych?

OK

Anuluj

**„Usuń Dane” program zapisze kopię danych do pliku json – i zapyta 2 razy o zgodę na usunięcie.**

**„Eksportuj Dane” program zapisze kopię danych do pliku json**