Backend logika

Flow web aplikácie – Asymetrická kryptografia:

1. Používateľ si dá vygenerovať Public a Private Key. Uloží si ich u seba.
2. Používateľ chce súbor zašifrovať. Spolu so súborom nahrá aj svoj Public Key.

* Na servery sa vygeneruje Secret Key
* Secret Key zašifruje súbor
* Secret Key sa zašifruje pomocou Public Key
* Zašifrovaný súbor a zašifrovaný Secret Key sa pošlú späť (zatiaľ iba v response headry)

1. Používateľ chce súbor dešifrovať. Spolu so súborom nahrá aj svoj Private Key. (Keď Secret Key nie je súčasťou súbora musí nahrať aj ten – TODO)

* Secret Key sa dešifruje pomocou Private Key
* Dešifrovaný Secret Key dešifruje súbor
* Dešifrovaný súbor sa pošle späť

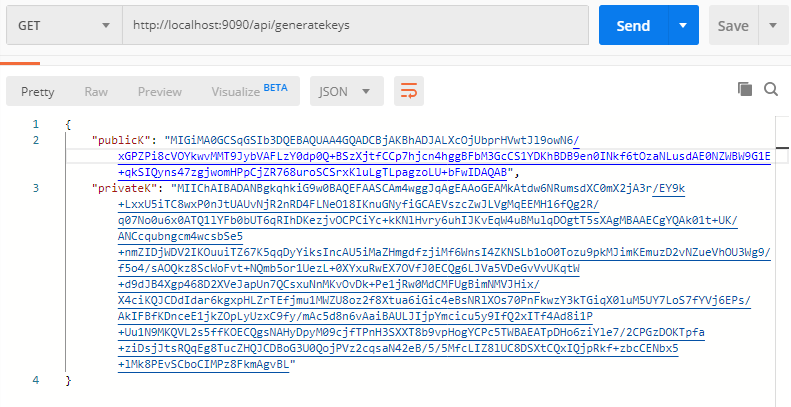
1. Používateľ si vygeneruje nový Public a Priv Key

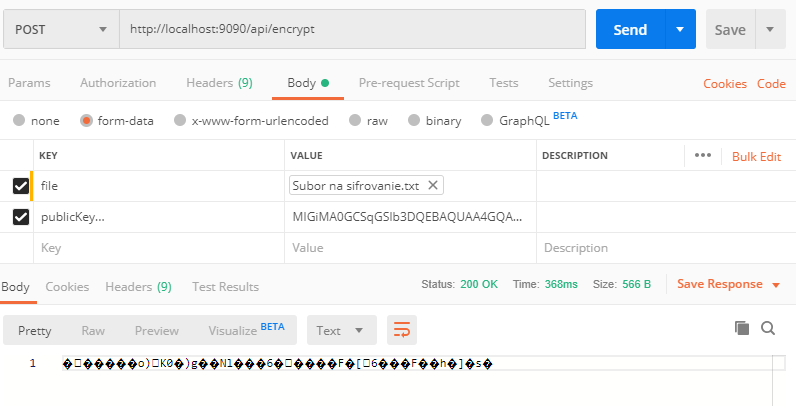
TODO:

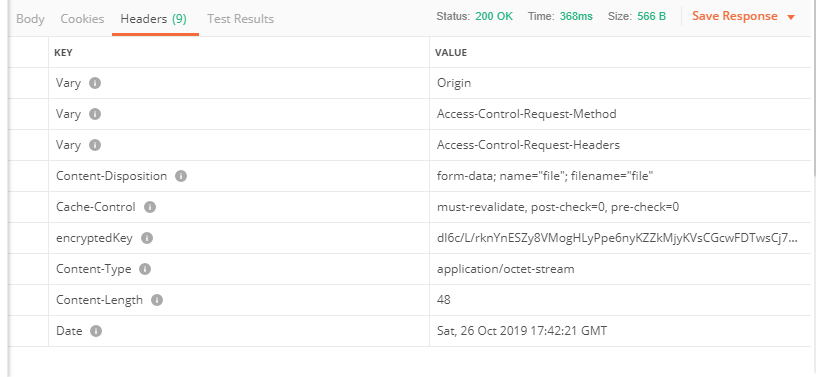
* Kontrola integrity
* Nekontroloval som vôbec tie typy šifier – môžu byť neaktuálne
* Posielanie Secret Key ako súčasť zašifrovaného súboru
* Offline aplikácia na dešifrovanie

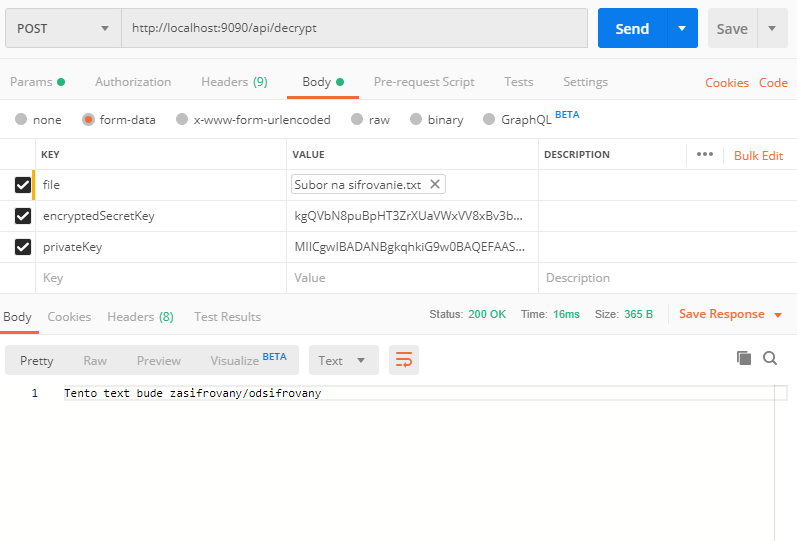
Ukážka pre frontend:

1)









API

Endpointy

* /api/generatekeys
* /api/encrypt
* /api/decrypt