

PREČO TÁTO PRÁCA VZNIKLA?

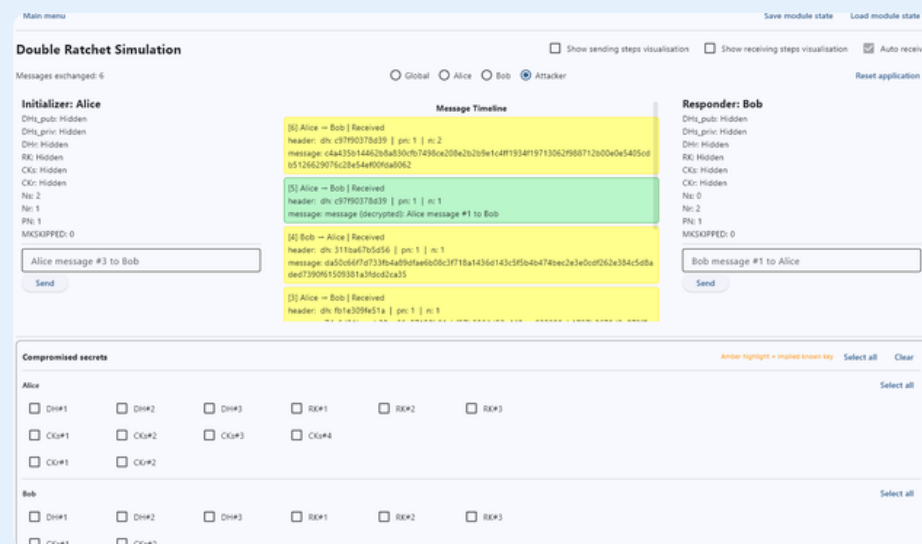
Signal protokol využíva komplexné kryptografické mechanizmy, ktoré sa ťažko chápu iba zo špecifikácií. Cieľom práce bolo vytvoriť interaktívny edukačný nástroj, ktorý tieto procesy vizualizuje a umožňuje nimi prechádzať krok za krokom.

ČO APLIKÁCIA PONÚKA?

Aplikácia umožňuje interaktívne simulovať a vizualizovať:

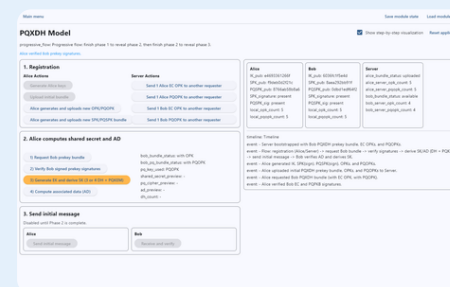
- **X3DH** – vytvorenie počiatočného zdieľaného tajomstva
- **PQXDH** – post-kvantovú alternatívu k X3DH
- **Double Ratchet** – priebežnú obnovu kľúčového materiálu pri komunikácii
- **SPQR / SCKA** – post-kvantové zabezpečenie ratchet mechanizmu
- **Triple Ratchet** – kombináciu klasického Double

Používateľ môže jednotlivými operáciami prechádzať krok za krokom, sledovať zmeny kľúčového materiálu a pozorovať stav jednotlivých účastníkov komunikácie.

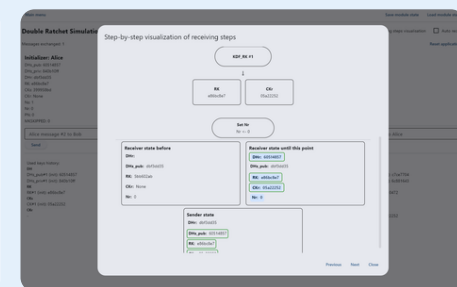


HLAVNÝ PRÍNOS

Most medzi formálnou špecifikáciou Signal protokolu a jeho praktickým pochopením. Používateľ môže sledovať kľúče, stav komunikácie, jednotlivé kroky ratchetov aj dôsledky kompromitácie a následnú Post-Compromise Security



Modul PQXDH znázorňuje proces postkvantovej dohody o kľúči a vymenený kľúčový materiál.



Vizualizácia procesu prijímania krok za krokom so zvýraznenými zmenami a synchronizovanými kľúčovými hodnotami