

CryMe  
PB173 Projekt

Antonín Dufka, Štěpánka Gennertová

12.3.2018

# Úvod

Aplikace CryMe bude sloužit k výměně zašifrovaných zpráv mezi uživateli skrze centrální server. Síťová komunikace bude probíhat skrze TCP spojení iniciovaná klienty.

## Možnosti uživatele

- ▶ vygenerování dvojice klíčů pro asymetrickou komunikaci
- ▶ zaregistrování se do aplikace na základě veřejného klíče a pseudonymu
- ▶ přihlášení se k serveru
- ▶ navázání spojení s jiným uživatelem
- ▶ šifrovaná komunikace s jiným uživatelem (výměna zpráv)
- ▶ ukončení spojení se serverem
- ▶ pamatování si uživatelů, se kterými se už spojil

# Kryptografie

K zajištění bezpečnosti využíváme

- ▶ RSA-2048 pro asymetrickou kryptografii (při iniciální komunikaci mezi serverem a klientem)
- ▶ challenge - response protokol pro autentizaci klienta i serveru (na jehož základě se vygeneruje klíč pro následovnou symetricky šifrovanou komunikaci)
- ▶ SHA2-256 pro vytvoření symetrického klíče (pro každé spojení se generuje nový)
- ▶ další komunikace mezi klientem a serverem je šifrována AES-256

# Server

## Funkcionalita serveru

- ▶ zaregistrování uživatele - jeho pseudonymu a veřejného klíče
- ▶ drží si databázi pseudonymů a veřejných klíčů uživatelů (příp. i symetrického klíče)
- ▶ autentizace uživatele
- ▶ poskytnutí uživateli veřejný klíč jiného uživatele podle zadaného pseudonymu
- ▶ přeposílání zpráv mezi uživateli
- ▶ ukončení TCP spojení s uživatelem