Laboratorium nr 4-5: Onion routing

Język programowania: dowolny

Zadanie:

Celem zadania jest zaimplementowanie programu demonstrującego zasadę działania trasowania cebulowatego służącego do zapewniania anonimowości transmisji danych. Należy napisać dwa programy klient i przekaźnik.

Ważne: Przed przystąpieniem do wykonania zadania zapoznaj się z zasadami trasowania cebulowatego z wykładu.

- **Klient:**
  - Klient ma umożliwić pobranie dowolnego pliku z dowolnej strony WWW i zapisanie go na dysku.
  - Klient ma posiadać interfejs graficzny (UI).
  - Klient z pliku na dysku odczytuje listę adresów IP oraz portów przekaźników i wyświetla na jednym z pól UI.
  - Klient wybiera 3 przekaźniki i szyfruje kolejno ich kluczami symetrycznymi adres URI żądanego pliku (w celu uproszczenia zadania klient może znać wcześniej współdzielony klucz symetryczny z każdym przekaźnikiem (np. można zapisać klucze w pliku z adresami IP)).
  - Zaszyfrowany plik wysyłany jest do pierwszego przekaźnika. Następnie klient oczekuje na informacje zwrotną od przekaźnika, którą jest zaszyfrowany, pobrany plik. Odszyfrowywanie następuje w kolejności odwrotnej do szyfrowania.
- **Przekaźnik:**
  - Działa w trybie tekstowym, po uruchomieniu oczekuje na połączenia od klientów i przekaźników.
  - Dane są odszyfrowywane i w przypadku, gdy zawartość odszyfrowana zawiera żądanie pobrania, przekaźnik pobiera żądany plik, w przypadku gdy dane mają zostać przekazane dalej odczytuje adres IP, port kolejnego przekaźnika i przekazuje dane dalej.
  - Przekaźnik końcowy po pobraniu pliku szyfruje go swoim kluczem i odsyła do przekaźnika od którego go dostał; przekaźniki pośrednie robią to samo, po otrzymaniu informacji zwrotnej szyfrują ja swoim kluczem i odsyłają z powrotem.