Počítačové siete - Šifrovaná komunikácia :)

Komunikácia, ktorej utajenie obsahu je zabezpečené šifrovaním.

Bezpečnosť prenosu údajov sa v počítačovej sieti štandardne rieši prostredníctvom **SSL** (ktorá predstavuje súčasne vrstvu aj protokol). Jedným z najčastejšie používaných protokolov je **HTTPS**.

Vytvorenie spojenia prebieha prostredníctvom asymetrického šifrovania, kde používateľ v prvom kroku požiada server, s ktorým chce komunikovať, o doručenie asymetrického verejného kľúča a určenie kryptovacieho algoritmu symetrického kľúča, prostredníctvom ktorého bude prebiehať komunikácia. Server kľúč odošle spolu s **bezpečnostným certifikátom**, ktorý slúži na overenie jeho totožnosti a hodnovernosti.

V prípade, že používateľ certifikát akceptuje, vygeneruje jeho systém unikátny symetrický kľúč, na základe ktorého bude prebiehať ďalšia komunikácia, zašifruje ho verejným asymetrickým kľúčom servera a výsledok mu pošle.

Server svojím (asymetrickým) súkromným kľúčom prijaté údaje dešifruje a potvrdí používateľovi. V tomto momente obaja účastníci komunikácie disponujú symetrickými kľúčmi pre kryptovanú komunikáciu a môže začať prenos údajov. Dôvodom prečo sa používajú dva spôsoby šifrovanie je, že asymetrické šifrovanie je oveľa pomalšie a náročnejšie na výpočet, kvôli čomu ho nemožno použiť na permanentný prenos rozsiahlych údajov.

Bezpečnosť v sieti ↑

Bezpečnostný certifikát ↓

Copyright © 2013 - 2025 Encyklopédia poznania