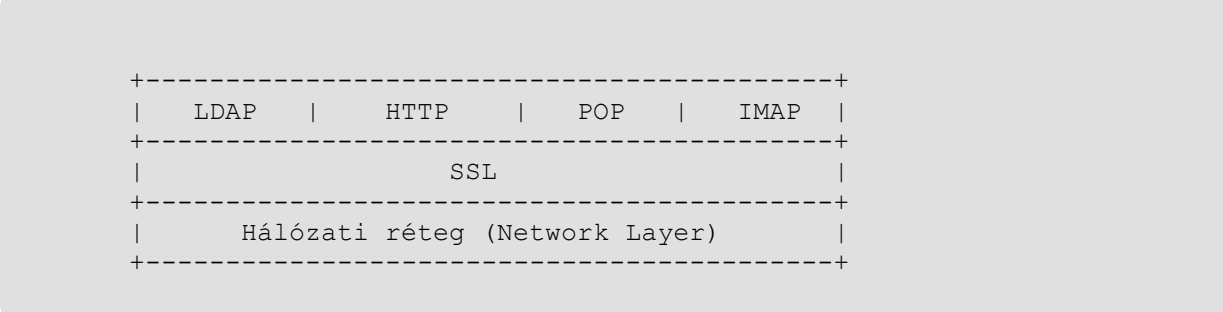
Az SSL

Az SSL (Secure Socket Layer; Biztonsági Alréteg) egy protokoll réteg, amely a hálózati (Network layer) és az alkalmazási rétegek (Application layer) között van. Mint neve is sugallja, az SSL mindenféle forgalom titkosítására használható - LDAP, POP, IMAP és legfőképp HTTP.

Íme egy végletekig leegyszerűsített ábra az SSL-el kapcsolatban álló rétegekről.



Az SSL-ben használt titkosító algoritmusok

Háromféle titkosítási technológiát használnak az SSL-ben: "nyilvános-titkos kulcs" (Public-Private Key), "szimmetrikus kulcs" (Symmetric Key), és "digitális aláírás" (Digital Signature).

"Nyilvános-titkos kulcs" titkosítás - SSL kapcsolat indítása: Ebben az algoritmusban a titkosítás és a visszafejtés nyilvános-titkos kulcspárral történik. A webszerveré a titkos kulcs, a nyilvános kulcsot pedig a tanúsítványban küldi el a kliensnek.

1. A kliens kéri a HTTPS-t használó Web szervertől a tartalmat.
2. A web szerver válaszol egy Digitális Tanúsítvánnyal (Digital Certificate), amiben benne van a szerver nyilvános kulcsa.
3. A kliens ellenőrzi, hogy lejárt-e a tanúsítvány.
4. Ezután a kliens ellenőrzi, hogy a tanúsítvány hatóság (Certificate Authority; továbbiakban CA), amely aláírta a tanúsítványt, megbízott hatóság-e a böngésző listáján. Ez a magyarázata annak, miért van szükségünk egy megbízott CA-tól kapott tanúsítványra.
5. A kliens ellenőrzi, hogy a webszerver teljes domain neve (Fully Qualified Domain Name) megegyezik-e a tanúsítványon lévő közönséges névvel (Common Name).
6. Ha minden megfelelő, létrejön az SSL kapcsolat.

Bármi, amit titkos kulccsal titkosítottak, kizárólag a nyilvános kulccsal fejthető vissza. Ennek megfelelően, bármilyen nyilvános kulccsal titkosított dolog, kizárólag a titkos kulccsal fejthető vissza. Elterjedt az a tévhit, miszerint kizárólag nyilvános kulccsal lehet titkosítani és titkos kulccsal visszafejteni. Ez nem így van. Bármelyik kulcs használható titkosításra és visszafejtésre egyaránt (ha annak párját használják visszafejtésre és titkosításra - dacas). Végül is, ha az egyik kulcsot használták titkosításra, a másikat kell használni a visszafejtésre stb. Egy üzenet nem titkosítható és visszafejthető kizárólag a nyilvános kulcs használatával.

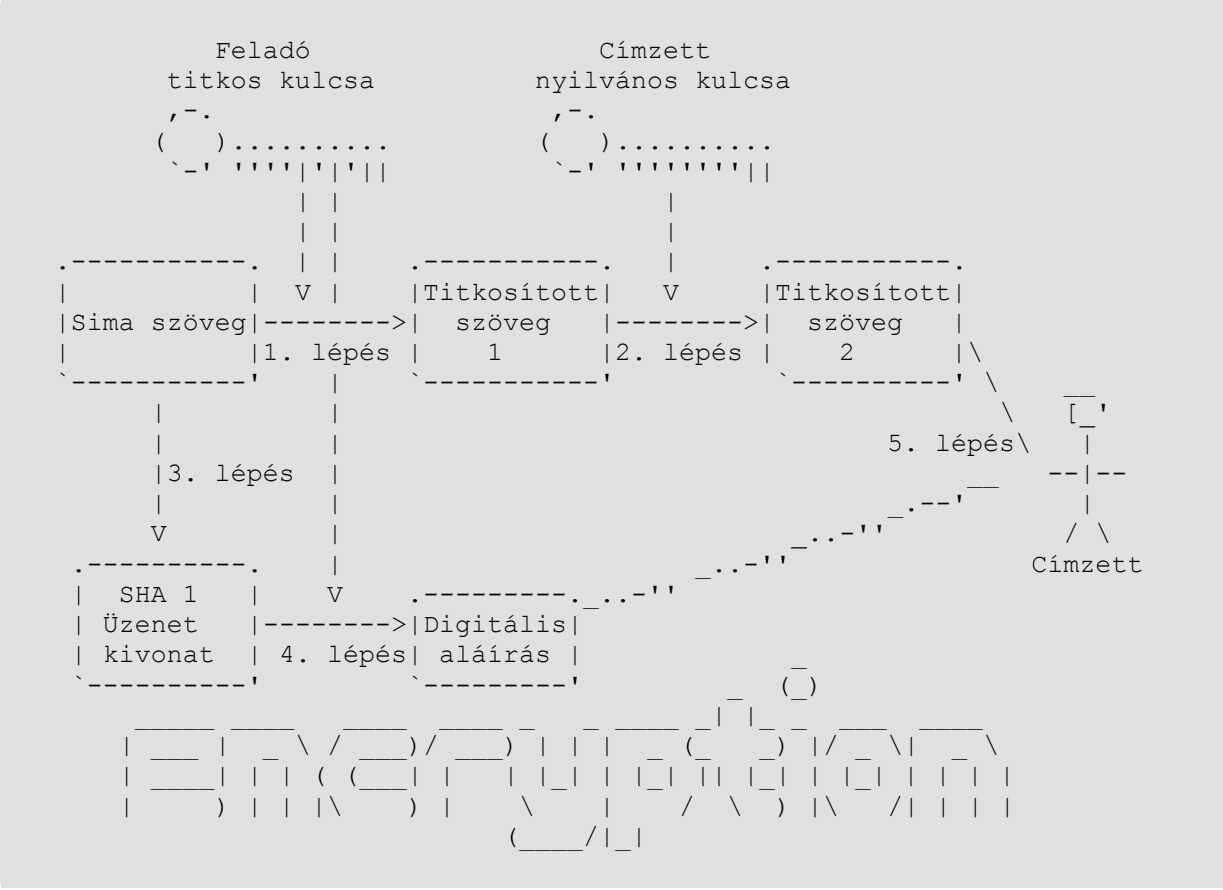
A titkos kulccsal történő titkosítás és a nyilvános kulccsal történő visszafejtés biztosíték a címzetteknek arról, hogy a küldeményt a küldő (a titkos kulcs tulajdonosa) adta fel (mivel a titkos kulcs használatához szükséges jelmondatot csak Ő ismeri - dacas). A nyilvános kulccsal történő titkosítás és titkos kulccsal visszafejtés biztosítja azt, hogy a küldeményt csak a meghatározott címzett (a titkos kulcs tulajdonosa) képes visszafejteni.

Szimmetrikus titkosítás - az adatok tulajdonképpeni átvitele: Miután az SSL kapcsolat létrejött, szimmetrikus titkosítást használ az adatok titkosítására, kevesebb CPU ciklust felhasználva (tehát kevésbé erőforrás igényes). Szimmetrikus titkosításkor az adat ugyanazzal a kulccsal titkosítható és visszafejthető. A szimmetrikus titkosítás kulcsa a kapcsolat indításakor kerül átadásra, a nyilvános-titkos kulcspárral történő titkosítás alatt.

Üzenet ellenőrzés A szerver kivonatot készít az üzenetről valamilyen algoritmus szerint, mint például HMAC, SHA, MD5, majd ezek alapján ellenőrzi az adatok sértetlenségét.

A hitelesség és sértetlenség ellenőrzése

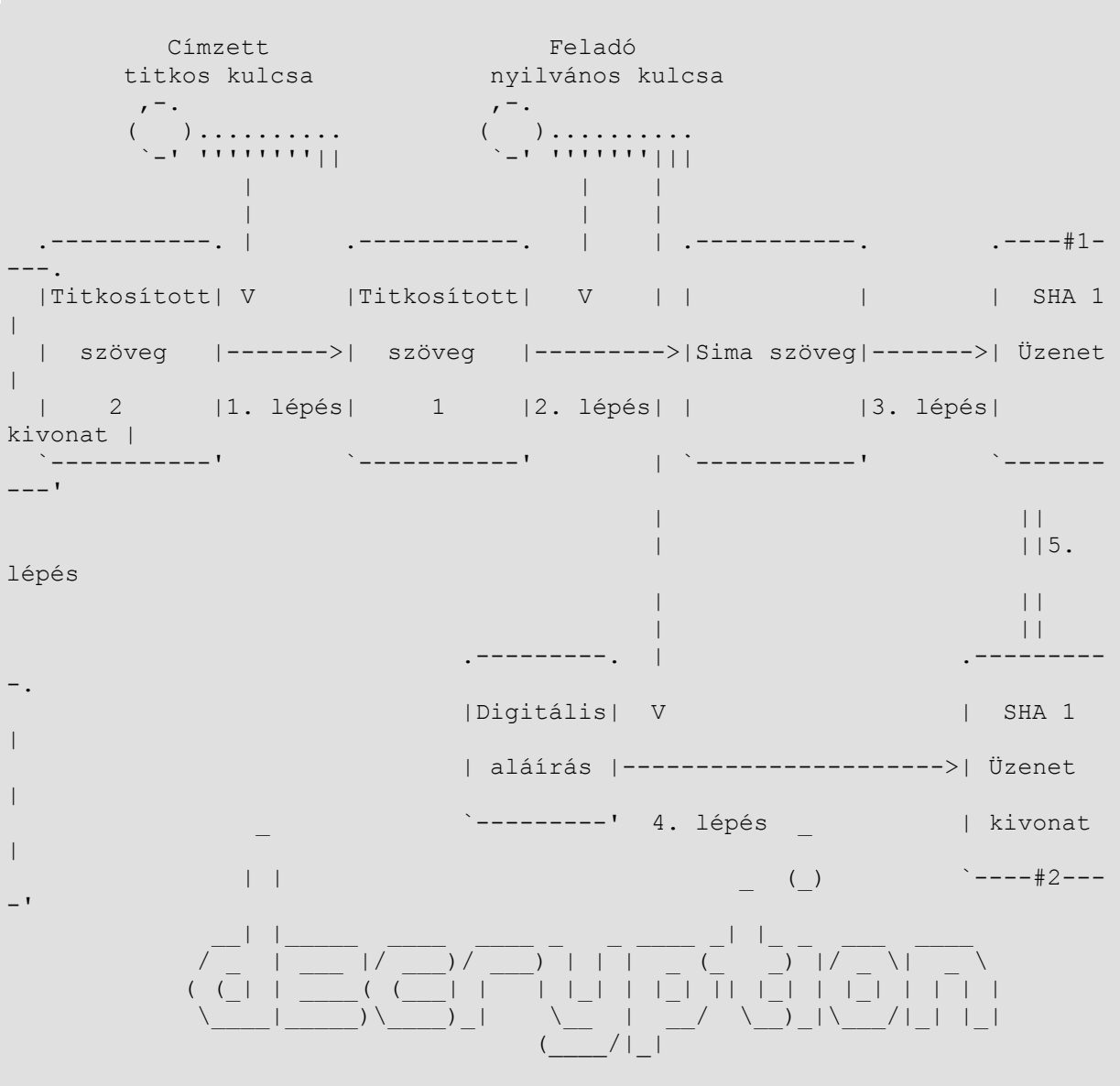
Titkosítási folyamat



- 1. lépés: az eredeti "sima szöveg" titkosítása a feladó titkos kulcsának használatával, ennek eredménye a "titkosított szöveg 1". Ez biztosítja a feladó hitelességét.
- 2. lépés: a "titkosított szöveg 1" titkosítása a címzett nyilvános kulcsával, ennek eredménye a "titkosított szöveg 2". Ez biztosítja a címzett hitelességét (értsd: csak a címzett tudja visszafejteni a szöveget a saját titkos kulcsával).

- 3. lépés: az SHA1 üzenet kivonat (ellenőrző összeg - dacas) készítése a "sima szöveg" alapján.
- 4. lépés: SHA1 üzenet kivonat titkosítása a feladó titkos kulcsával, ennek eredménye a "sima szöveg" digitális aláírása. Ezt a digitális aláírást a címzett felhasználhatja az üzenet sértetlenségének és a feladó hitelességének ellenőrzésére.
- 5. lépés: a "digitális aláírás" és a "titkosított szöveg 2" elküldése a címzettnek.

Visszafejtési folyamat



- 1. lépés: a "titkosított szöveg 2" visszafejtése a címzett titkos kulcsának használatával, ennek eredménye a "titkosított szöveg 1".
- 2. lépés: a "titkosított szöveg 1" visszafejtése a feladó nyilvános kulcsának használatával, ennek eredménye a "sima szöveg".
- 3. lépés: SHA1 üzenet kivonat (ellenőrző összeg - dacas) elkészítése, az előző 2 lépés eredményeként kapott "sima szöveg" alapján.
- 4. lépés: a "digitális aláírás" visszafejtése a feladó nyilvános kulcsának használatával, ennek eredménye az "SHA1 üzenet kivonat".

- 5. lépés: az "SHA üzenet kivonat #1" és "SHA üzenet kivonat #2" összehasonlítása. Amennyiben a kettő egyezik, úgy az üzenet nem módosult az átvitel alatt, így az eredeti "sima szöveg" sértetlen.

Tanúsítványok

Használathoz szükségünk lesz egy tanúsítványra valamely Certificate Authority-tól (tanúsítvány hatóság) (ezentúl CA). A CA-k a tanúsítványt áruba bocsátók, akik egy megbízható CA listán vannak a felhasználó böngésző kliensében. Mint azt az algoritmus titkosítás részben említettem, ha a CA nincs a megbízott hatóságok listáján, a felhasználó figyelmeztető üzenetet kap, amikor megpróbál kapcsolódni egy biztosított/biztonságos helyhez.