Bejelentkezés Nyilvános kulcsú titkosítás segítségével

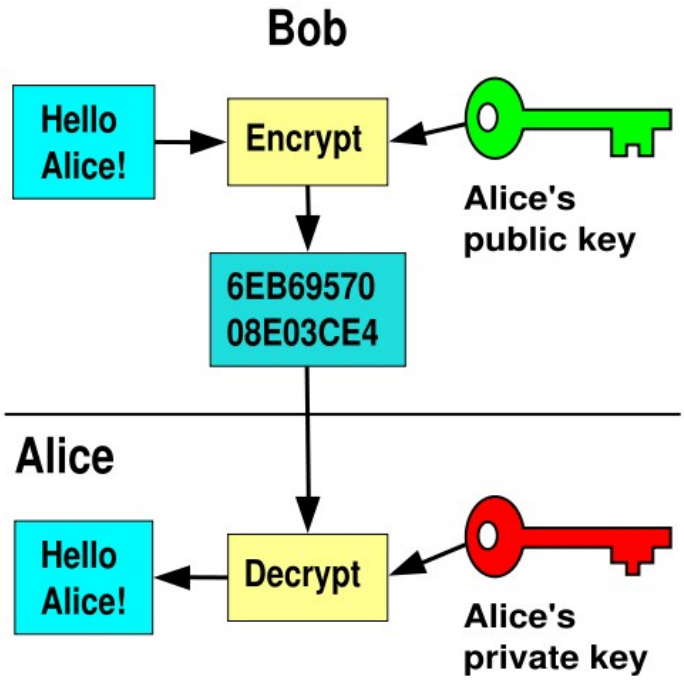
Mivel a tárgynak nem célja kimerítően foglalkozni a témával, ezért csak egy pár szóból álló gyorstalpalót olvashattok itt a nyilvános kulcsú titkosításról.

A nyilvános kulcsú titkosítás az aszimmetrikus titkosítások családjába tartozik, hogy mit is jelent ez, azt legkönnyebben a szimmetrikus titkosításon keresztül lehet megérteni. Szimmetrikus titkosítás esetén van egy darab titkos kulcs, amit a titkosításban részvevő felek *előre* megosztanak egymással. Ennek hátrányai azonnal láthatóak: mi történik, ha az egyik féltől ellopják ezt a kulcsot? Illetve hogyan oldjuk meg, hogy az éppen aktuális kulcs anélkül eljusson a részvevőkhöz, hogy tartalma nyilvánossága kerüljön?

Ez alapján az aszimmetrikus titkosítás alapötlete az, hogy az a kulcs, amit a titkosításra használunk nem egyezik meg azzal a kulccsal, amit a titkosítás feloldására használunk. A következő ábrákon Alice és Bob történetén keresztül vizsgáljuk meg a nyilvános kulcsú titkosítást.

A felállás a következő: Adott Alice és Bob, akik szeretnének egy mással levelezni, de azt, hogy mit leveleznek, nem szeretnék mások orrára kötni. Tovább adott még 2-2 darab kulcspár. Alice rendelkezik egy ***titkos*** és egy ***publikus*** kulccsal. A titkos kulcsát egy biztonságos helyen őrzi, de nyilvános kulcsát nyugodtan elküldheti barátainak, vagy felrakhatja az internetre. Bob is rendelkezik egy ***titkos*** és egy ***publikus*** kulcspárral.

Amikor Bob szeretne üzenetet küldeni Alice-nek, mint az alább „Hello Alice!” tartalommal, akkor az üzenetét Alice ***publikus*** kulcsával titkosítja, ez azt garantálja, hogy az üzenetet csak Alice tudja vissza fejteni.

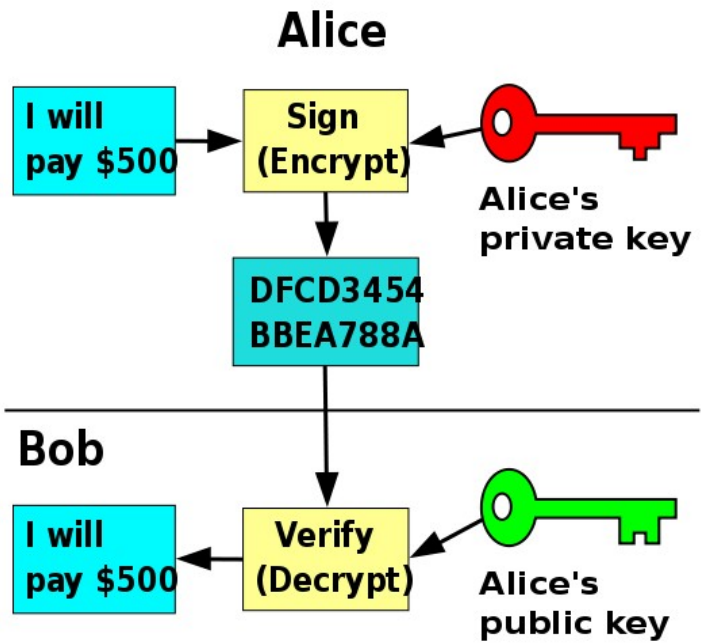


Amikor Alice postafiókjába megérkezik a kódolt levél, saját biztos helyen őrzött titkos kulcsával vissza tudja fejteni az üzenetet, mivel azt az Ő saját nyilvános kulcsával titkosították.

Van egy másik felhasználási módja is a nyilvános kulcsú titkosításoknak: ez pedig a hitelesítés, vagy más néven digitális aláírás. Ebben felállásban Bob szeretne biztos lenni, hogy amit kapott e-mailt azt valóban Alice küldte, és nem más ígért neki 500 dollárt Alice nevében.

A fenitek megvalósítása a következő:
Alice ír egy levelet, majd itt két lehetőség adódik: vagy Alice tikosítja az üzenetét, mint az előzőekben, vagy készít a levél tartalmából egy **aláírás**t.

Titkosítás esetén a levél tartalmát csak az tudja elolvasni, aki rendelkezik Alice nyilvános kulcsával, hiszen az a privát kulccsal lett lekódolva. Aláírás esetén a címzett a levélhez fűzött egyedi aláírást tudja ellenőrizni, hiszen ha ezt a levélaláírást megfelelően tudja kikódolni, akkor valóban Alice küldte a levelet és a levél tartalma nem változott meg!
Tehát, itt két fontos nyereség van, az egyik a ***feladó kilétének garantálása*** a másik pedig az ***üzenet tartalmának sértetlensége***.



A célunk, hogy a fentieket felhasználva, jelszó megadása nélkül hozzunk létre ssh kapcsolatot helyi gépünk és egy távoli gép között.

Már csak azt kell tisztáznunk, hogy Alice és Bob példáját hogyan tudnánk átültetni a kliens szerver kapcsolatok világára. Hova kerüljön a titkos kulcs és hova a nyilvános, illetve kinek a kulcsára van szükség és hol?

Mivel a titkos kulcs mindig a tulajdonosnál kell, hogy legyen azt kiadni nem szabad, ezért az alapelv a következő. Amikor be szeretnénk jelentkezni egy távoli gépre jelszó használata nélkül, akkor el kell helyeznünk a távoli gépen a saját nyilvános kulcsunkat. Mivel ezt mi helyeztük el ezért jogosultak vagyunk bejelentkezni arra a távoli gépre, más részt mivel ez a saját titkos kulcsunk nyilvános párja, ezért biztos lehet a szerver, hogy mi jelenetkezünk be, hiszen visszatudja fejteni az üzenetünket a nyilvános kulcsunk segítségével.

http:

Cél hogy egy kicsit a böngésző működése mögé nézzünk.
Hogy azok a színes szagos honlapok mögött bizony egy szöveges állomány van, és a böngészőnk "beszélget" a http szerverrel.
Nézzünk meg egy honlapot a böngészőben úgy hogy megjelenítjük az "oldal forrása" paranccsal (firefox esetén CTRL+U)

ennek bemutatására csak egy egyszerű konzolos példa:

betelnetezünk valamelyik http szerverre (nem nehéz találni egyet) de pl lehet a www.itk.ppke.hu

Ezt windows-os konzolból is és linuxosból is csinálhatjuk, mindegy

```
user@user-laptop:~$ telnet www.itk.ppke.hu 80
Trying 193.225.109.11...
Connected to www.itk.ppke.hu.
Escape character is '^]'.
GET /index.html HTTP/1.1
host: www.itk.ppke.hu
<soremelés(enter)>

HTTP/1.1 200 OK
Date: Sun, 27 Sep 2009 18:26:40 GMT
Server: Apache
Last-Modified: Mon, 18 Aug 2008 12:44:46 GMT
ETag: "172f9-c79-560aab80"
Accept-Ranges: bytes
Content-Length: 3193
Cache-Control: max-age=7200, must-revalidate
Expires: Wed, 07 Oct 2009 18:26:40 GMT
Vary: Accept-Encoding
```

```
Content-Type: text/html; charset=UTF-8

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<HTML>
<HEAD>
   <META name="Author" content="PPKE-ITK">
   <META name="description" content="Peter Pazmany Catholic University
- Faculty of Information Technology">
    <META name="keywords" content="Peter Pazmany Catholic University
Faculty of Information Technology Pázmány Péter Katolikus Egyetem
Információs Technológiai Kar">
   <meta http-equiv="Content-Type" content="text/html; charset=utf-8">
   <TITLE>Pázmány Péter Katolikus Egyetem</TITLE>

   <link rel="stylesheet" href="index.css" type="text/css">

</HEAD>
<BODY>
......

</body>
</HTML>
```

Nézegessük a
http://www.w3.org/Protocols/rfc2616/rfc2616.html
oldalt, ahol a HTTP/1.1 leírása található

http vs. https:

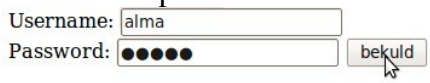
Mi a kulonbseg nagyvonalakban a http és a https közt?

A különbség szemléltetése:

próbáljuk ki a következő oldalt:
http://wsn.itk.ppke.hu/~tisda/szamtech_form/index.php

NE HASZNÁLJUNK VALÓDI FELHASZNÁLÓNEVET VAGY JELSZÓT

Először ezt az oldalt nézzük meg, írjunk be két értéket, és közben figyeljük wiresharkkal egy capture-t (vagy tcpdumppal, ahogy jobban tetszik) hogy hogy látszik a hálózaton plain textben a küldött infó annak ellenére, hogy a böngésző pöttyöket jelenített meg.
A wiresharkra egy olyan filtert célszerű tenni mondjuk hogy "host wsn.itk.ppke.hu" hogy a többi forgalmat ne vegye fel, így látható lesz ha csak ezt az oldalt használjuk hogy mi a menete a http szerver és kliens kommunikációjának.



Note that when you type characters in a password field, the browser displays asterisks or bullets instead of the characters.

```
user@user-laptop:~$ tcpdump -X -s1024 host wsn.itk.ppke.hu and port 80
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 1024 bytes
14:44:28.820425 IP r224-8.itk.ppke.hu.54755 > wsn.itk.ppke.hu.www: S 2350768946:2350768946(0)
win 5840 <mss 1460,sackOK,timestamp 19956133 0,nop,wscale 6>
        0x0000:  4500 003c 6297 4000 4006 9d4a 0a03 136a  E..<b.@.@..J...j
...
14:44:28.820605 IP wsn.itk.ppke.hu.www > r224-8.itk.ppke.hu.54755: S 1861501465:1861501465(0)
ack 2350768947 win 5792 <mss 1460,sackOK,timestamp 56388572 19956133,nop,wscale 6>
        0x0000:  4500 003c 0000 4000 4006 ffe1 0a03 136b  E..<..@.@......k
...
```

```
14:44:28.820645 IP r224-8.itk.ppke.hu.54755 > wsn.itk.ppke.hu.www: . ack 1 win 92
<nop,nop,timestamp 19956133 56388572>
        0x0000:  4500 0034 6298 4000 4006 9d51 0a03 136a  E..4b.@.@..Q...j
...
14:44:28.820900 IP r224-8.itk.ppke.hu.54755 > wsn.itk.ppke.hu.www: P 1:596(595) ack 1 win 92
<nop,nop,timestamp 19956133 56388572>
        0x0000:  4500 0287 6299 4000 4006 9afd 0a03 136a  E...b.@.@......j
...
        0x0260:  2d4c 656e 6774 683a 2032 340d 0a0d 0a75  -Length:.24....u
        0x0270:  7365 723d 616c 6d61 2670 6173 7377 6f72  ser=alma&passwor
        0x0280:  643d 6b6f 7274 65                        d=korte
14:44:28.821280 IP wsn.itk.ppke.hu.www > r224-8.itk.ppke.hu.54755: . ack 596 win 110
<nop,nop,timestamp 56388572 19956133>
        0x0000:  4500 0034 29c6 4000 4006 d623 0a03 136b  E..4).@.@..#...k
...
14:44:28.824092 IP wsn.itk.ppke.hu.www > r224-8.itk.ppke.hu.54755: P 1:620(619) ack 596 win
110 <nop,nop,timestamp 56388573 19956133>
        0x0000:  4500 029f 29c7 4000 4006 d3b7 0a03 136b  E...).@.@......k
...
14:44:28.824131 IP r224-8.itk.ppke.hu.54755 > wsn.itk.ppke.hu.www: . ack 620 win 111
<nop,nop,timestamp 19956134 56388573>
        0x0000:  4500 0034 629a 4000 4006 9d4f 0a03 136a  E..4b.@.@..O...j
...
```

majd ugyan így használjuk a https kapcsolaton keresztül UGYAN EZT a formot:

https://wsn.itk.ppke.hu/~tisda/szamtech_form/index.php

szintén capture wiresharkkal, vagy tcpdumppal és lám, nem lehet látni a küldött üzeneteket.