

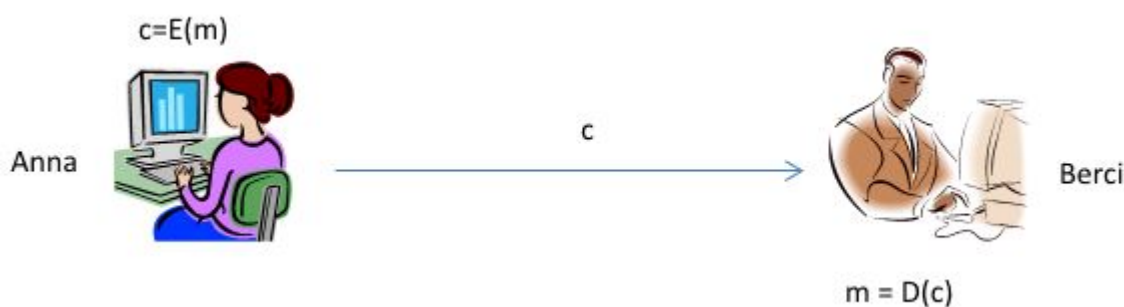
Kriptográfia

A kriptográfia szó görög eredetű: (κρυπτός (kryptós) azaz 'rejtett', γράφειν (gráphein) = 'írás') jelentése: titkosítás. Ez a témakör mára önállóvá vált, de elsősorban informatikai tudományág, amely a titkosítással és azok megfejtésével, megfejthetőségével foglalkozik. Az elektronikus kommunikáció elterjedésével három alapkövetelmény jelenik meg a titkosítások módszerével, használatával szemben, aminek alkalmazásával például egy biztonságos internetes kommunikációs csatorna valósulhat meg:

Biztonságos csatorna alapkövetelményei:

- **titkosság:** a kommunikáló feleken kívül más ne ismerhesse az üzenetek tartalmát. Eszköz: **rejtjelező algoritmus**. Célunk itt sokrétű, olyan módszert kell alkalmazni, amely egyszerre visszafejthetetlen, gyorsan számolható, kényelmesen alkalmazható. Bizonyítani kell matematikai úton, hogy melyek a módszer határai.
- **hitelesség:** a kommunikáló felek meggyőződhetnek egymás személyazonosságáról. (akár anélkül is, hogy bármikor találkoztak volna) Eszközök: **hitelesítő szolgáltatás** (hatóságok). Természetes igény az internetes kommunikáció során, hogy olyan távoli szerverekkel kell megbízhatóan kommunikálni, amelyeket képtelenség megközelíteni, mégis biztosítani kell olyan algoritmust, amely segít a személyazonosság garantálásában. 100%-os biztonság nincs, de jelen esetben is ismerni kell a határokat.
- **integritás:** meg kell gátolni az adataink észrevétlen megváltoztatását. Eszköz: digitális aláírás. Manapság olyan digitális "szerződéseket" is kell kötnünk, amely során nem lehetnek a felek jelen. Sőt az aláírások ideje is nem azonos időben történik. A digitális aláírás ma már Magyarországon is kötelező számos területen, pl. a cégbírósági ügyintézéskor.

A kommunikáció alapmodellje és jelölései:



Ahol, **Anna:** a küldő fél (A), **Berci:** a fogadó fél (B),

m: üzenet (message), **c:** kódolt üzenet (code),

E(): titkos kódoló függvény (encrypt),

D(): titkos dekódoló függvény,

az **E()** a **D()** inverze a visszafejtő függvény (decrypt).

From:
<https://edu.iit.uni-miskolc.hu/> - Institute of Information Science - University of Miskolc

Permanent link:
https://edu.iit.uni-miskolc.hu/tanszek:oktatas:infrendalapjai_architekturak:informacio_titkositas_es_hitelesites:kriptografia

Last update: **2024/11/13 17:12**

