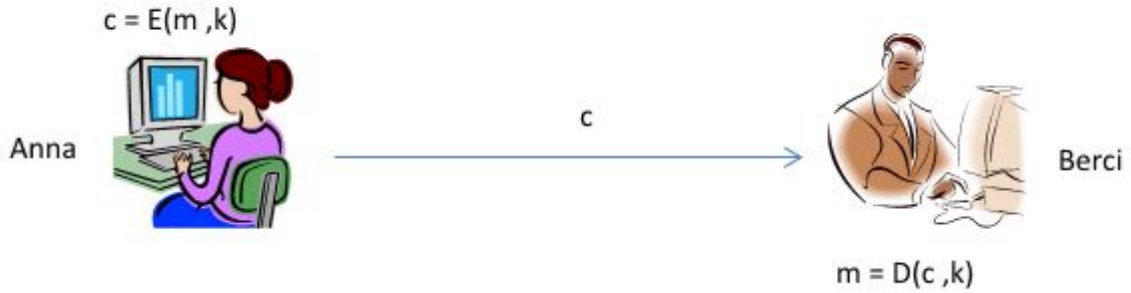
Kerckhoffs elv

Az alapmodell alkalmazása nehézkes, mert mindkettőjüknek tudni kell a **E()** és **D()** függvényeket, ami maga a titkosítási eljárás, ha a módszer kiderül, akkor a kommunikáció lehallgathatóvá válik. Sokkal egyszerűbb lenne a helyzet, ha olyan megoldásokat keresnének, amelyiknél az eljárás mindig ugyanaz, a biztonságot egy közösen használt **titkos kulcs** (k) adná, amit csak ketten ismernek.



A Kerckhoffs-elv, amelyet Auguste Kerckhoffs holland kriptográfus fogalmazott meg, a kriptográfia egyik alapelve, amely kimondja, hogy egy titkosítási rendszer biztonságát nem a használt algoritmus titkossága, hanem a titkos kulcs titkossága kell, hogy biztosítsa. Az elv lényege az, hogy egy kriptográfiai rendszer akkor biztonságos, ha még akkor is megőrzi biztonságát, ha mindenki ismeri az algoritmust, kivéve a titkos kulcsot.

Az elvet többféleképpen szokták megfogalmazni, de a főbb gondolatok a következők:

- **Nyílt algoritmusok használata**: az algoritmus maga nem titkos. Bárki hozzáférhet az algoritmushoz, és azt megvizsgálhatja. A biztonságot a titkos kulcs rejti, amelyet csak a jogosult személyek ismernek. Nem jó az algoritmus, amelyik azért biztonságos, mert senki sem ismeri a működését, mivel előbb-utóbb úgyis kiderül hogyan működik, és az alkalmazóknak nagy kárt tud okozni. mindenki hallott már olyan újsághírekről, amelyben titokban őrzött módszereket egy középiskolás megfejtett.
- **Biztonsági garanciák a kulcson keresztül**: ha egy támadó hozzáfér az algoritmushoz, de nem ismeri a kulcsot, akkor nem képes megfejteni az üzenetet. Ha mindenki belátja az alkalmazott módszerről, hogy a visszafejtésben csak a “brute-force/nyers erő” módszer segít (ami minden lehetséges eset kipróbálását jelenti a gyakorlatban), akkor ilyen algoritmust érdemes alkalmazni, mivel belátható időn belül a visszafejtése lehetetlen.
- **Egyszerűség és hatékonyság**: a rendszer legyen egyszerű, hatékony és könnyen megvalósítható, hogy a gyakorlati alkalmazásokban könnyen használható legyen.

Összegezve: A Kerckhoffs-elv tehát azt jelenti, hogy a kriptográfiai rendszer akkor tekinthető biztonságosnak, ha az algoritmus nyilvános, és csak a titkos kulcs őrzi meg az adatok titkosságát.