Csirmaz László
Közép Európai Egyetem

Mennyire biztonságosak a kriptográfiai protokollok?

A 2005-ös év kriptográfiai szenzációja az MD5 elnevezésű kriptográfiai algoritmus (kivonatoló függvény) feltörése volt. Mind az MS Word, mind az MS Excel programok ezt használják az álományok azonosítására: a feltételezés szerint egy dokumentum változatlan ha a kivonat változatlan. Az említett kriptográfiai eredményt használva viszont könnyen állíthatunk elő két különböző dokumentumokat ugyanazzal a kivonattal.

Bízhatunk-e ezek után a kriptográfiai eljárásokban? Mi történik, ha idén az összes kriptográfiai eljárást feltörik? Ha a világ összes hacker-je összeáll és trójai falovakkal a világ összes számítógépét a titkos kulcsok megfejtésére használják? Mi történik amikor kvantumszámítógépeket olcsón lehet majd kapni, és az akárhány bites RSA-t percek alatt lehet fejteni?

A kriptológusok cseppet sem borulátók. A rendelkezésre álló több tucatnyi, alapvetően más elven működő kivonatoló, titkosító, szimmetrikus és aszimmetrikus algoritmusok közül bármelyikéről kiderülhet, hogy könnyen törhető. De "van másik" -- amelyik azonnal átveheti gyengének bizonyult társa feladatát.