TITKOSÍTSUNK!

A régebbi korok titkosírásának az volt a célja, hogy egy adott üzenetet eljuttassanak egy másik személyhez úgy, hogy azt csak ő értse meg. Az üzenet gyakran katonai, hadi műveleteket, vagy eltitkolt szerelmi kapcsolatok párbeszédét tartalmazta. Napjainkban ez a felhasználási terület visszaszorult, és a titkosítás célja az adatbiztonság lett. A mindennapi életünkben gyakran találkozunk az információk elektronikus tárolásával, továbbításával és feldolgozásával kapcsolatos feladatokkal, melyek egy része nem nyilvános. A számítástechnikában és a hírközlésben nagyon sok olyan kód van, melyek célja nem a titkosítás, hanem az adatok biztonságos tárolása vagy továbbítása.

Mondandónk rögzítésére írásjeleket használunk. A magyarok elődei és később a székelyek a rovásírás jeleit használták. Ha két ember úgy kommunikál egymással, hogy a kívülállók nem tudják értelmezni jelöléseiket, akkor ***titkosításról*** beszélünk.
Régóta gondja az embereknek, hogyan rejtsék el mondandójukat az illetéktelenek elől.

Kopogós titkosírás

A titkos üzenet betűit úgy kell továbbítani, hogy a soron következő betű oszlopának, majd sorának számát kopogtatjuk ki. Az R betű például először hat kopogás, utána négy kopogás.
A magyar ábécé 35 egyjegyű betűt tartalmaz, ezért egy hely látszólag üresen maradt. Ezt használjuk fel a szóköz írásához, hogy könnyebb legyen a visszafejtő dolga.
A rejtjelezett, más szóval kódolt szöveget le is lehet írni. Például számokat írunk: ezek első jegye (a tízesek) az oszlopot, míg a második jegy (az egyesek) a sort jelenti.

Az ókori titkosítások

Egyik formája volt, hogy leborotválták a rabszolga haját, és fejbőrére ráírták az üzenetet. A haja megnövéséig sötét, elzárt helyen tartották, majd elküldték a címzetthez, aki szintén leborotválta a rabszolga haját, és sötét, elzárt helyen tartotta.

Spártaiak titkosírását

Egy botra vékony bőrszíjat tekertek fel szoros menetekben. A szöveget egymást követő sorokban a szíjra írták, minden menetre egy-egy betűt. A letekert szíjon értelmetlen betűhalmaz sorakozott. Az írás csak akkor vált olvashatóvá, ha egy ugyanolyan vastagságú botra tekerték fel ismét a szíjat.

Ceasar-kód

A kommunikációnk során sokféle jelrendszert használunk, de ha ezt csak néhányan ismerik és használják információcserére, és a kívülállók nem értik, akkor titkosírásról beszélünk.

Az egyik titkosírási módszer a betűeltolás. A lényege az, hogy az ábécé betűit tetszőleges számú betűvel eltoljuk. A kódolás folyamán először el kell döntenünk, hogy milyen ábécét használunk (ékezetek, hosszú mássalhangzók szerepeljenek-e), majd azt, hogy hány betűvel toljuk el a kódolt ábécé betűit. Ezek után az ábécé betűit egy meghatározott számmal eltoljuk, és az eredeti ábécé alá írjuk. Így minden betűhöz rendeltünk egy másik betűt a titkos nyelvből, ami azonosítja, például az eredeti ábécében szereplő a betű helyett c betűt írunk, a b helyett d-t és így tovább. A titkos üzenet megírásakor egyesével vesszük az eredeti szövegbetűket, és helyére a titkosírásban szereplő betűpárját írjuk.

A dekódoláshoz tudnunk kell az adott ábécé típusát, és azt, hogy hány betűvel van eltolva. A titkosított szöveg betűit egyesével vesszük és az eredeti ábécé betűit hozzápárosítjuk, ezzel megkapjuk az eredeti információt.

A betűeltolás módszere Julius Caesar nevéhez fűződik. A legenda szerint ezzel az igen egyszerű, de hatékony titkosírási módszerrel kommunikált a légióival. Caesar nem küldött megfejtési kódot a titkos üzenet mellé, hanem közölte a célszeméllyel, hogy hány betűvel tolta el az ábécét a titkosírásban. A számot, vagyis a megoldás kulcsát futárokkal küldte, akik ezt versbe, vagy énekbe rejtették, és a címzettnek előadták.