HADMÉRNÖK

VII. Évfolyam 1. szám - 2012. március

Duka Péter
alltea3@gmail.com

AZ ITSO SZABVÁNYBAN ALKALMAZOTT NXP MIFARE KÁRTYÁK ELLEN ALKALMAZOTT TÁMADÁSI MÓDSZEREK

Absztrakt

Napjaink gyors fejlődésének köszönhetően a proximity kártyás olvasók egyre jobban beépülnek a mindennapokba, a világon mindenhol. Egyre modernebb, és biztonságosabb technológiákat fejlesztenek ki a tudósok és szakemberek. Azonban a fejlődéssel a „cyber világ" bűnözői lépést tartanak, erre jó példa a cikkben bemutatott nagybiztonságú Mifare kártyák elleni alkalmazott sikeres támadási módszerek.

Thanks to the quick development of the modern age, the proximity readers increasingly spread on the whole world. The scientists and specialists develops better and safer technologies. The criminalist of the cyber world keep up with the development, a good example for this is the attacks against the highly secure Mifare memory cards showed in this article.

Kulcsszavak: *proximity kártyás olvasó, Mifare kártya ~ proximity reader, Mifare memory card*

1. BEVEZETÉS

Az ITSO *(International Transport Smartcard Organization)* egy nonprofit célú szervezet, mely az ITSO specifikációk kidolgozásáért felelős, alapítása pedig egészen 1998-ig vezethető vissza. Az ITSO tehát egy nyílt szabványcsomagot nyújt, mely lehetővé teszi a felhasználók számára a tömegközlekedésben használatos elektronikus eszközök és rendszerek interoperábilis használatát. Az interoperabilitás azt jelenti, hogy egy adott országon belül, vagy akár más országokban egyetlen elektronikus kártya segítségével több szolgáltatás érhető el számunkra. Pl. egyetlen RFID *(Radio Frequency IDentification)* kártyánk elláthat bérlet funkciót és elektronikus pénztárca funkciót.

Az ITSO nyílt szabvány a következő szabványokra épül:

- ISO/IEC 7816: Kontaktussal rendelkező smart kártyákra vonatkozó szabvány.
- ISO/IEC 14443: Kontaktus nélküli (proxy) kártyákra vonatkozó szabvány.
- ISO/DIS 24014-1:Az interoperábilis közlekedési rendszer struktúrájára, és a rendszer menedzselésére vonatkozó szabvány.
- EN 1545: Adatelemekre, felépítésre vonatkozó szabvány.

Az ITSO alapjában véve az ISO/IEC 144431 A típusú szabványra épülő kártyák használatosak, – Pl. Mifare Classic 1K, DESFire, stb. -, de támogatja a B típusú, nagyobb biztonsággal rendelkező kártyákat is.

Továbbá az ITSO biztonsági modulja (SAM = Secure Application Module) megfelel a nemzetközileg elismert szabálygyűjtemény, a Common Criteria EAL 4-es megfelelési szintjének. Az EAL 4 szint jelentése: tervszerűen tervezve, tesztelve és megvizsgálva. (7 megfelelési szint létezik, minél nagyobb a szám annál költségesebb egy rendszer.)

A kártyák titkosítására a DES2 és 3DES-t alkalmazzák, ritkábban az AES3-t.

2. A KÁRTYÁKON ALKALMAZOTT TITKOSÍTÁSI FORMA BEMUTATÁSA

A legtöbb kártyán a szimmetrikus kulcsú DES[4] és 3DES titkosítást használják, ritkábban az AES[5]-t. Több célszámítógépet is kidolgoztak e kódok feltörésére. A feltöréshez szükséges idő egy DES titkosítás esetében mindössze néhány óra, ugyanakkor egy AES kód esetében a feltörés napjainkban még megoldhatatlan feladat.

A továbbiakban – az ITSO rendszereken belül túlnyomó részben alkalmazott *(a világon több mint 70%-ban használt)* – NXP *(Philips leányvállalata)* Mifare kártyákról lesz részletesebben szó, azon belül is a leggyakrabban használt Classic típusról. *(Fontos*

---

1 ISO/IEC 14443 specifikációk:
14443-2: modulációs eljárásra, és kódolásra vonatkozó sémák.
14443-3: ütközés elkerülésre (anti collison) vonatkozó sémák.
14443-4: kommunikációs protokoll leírása.

2 DES, 3DES: Data Encryption Standard
Szimmetrikus kulcsú kódolás. Manapság a DES megerősítését, a 3DES-t alkalmazzák, mely a DES kódolás végrehajtása 3-szor egymásután. Tehát az (X=1…3)DES sorra 64, 128 és 192 bites kulcsokat alkalmaz.

3 AES: Advanced Encryption Standard
Hivatalosan az USA Szabványügyi és Technológiai Intézete (National Institute of Standardisation and Technology) fogadta el 2001-ben, és váltotta le az elavultnak számító DES-t. Azonban továbbra is gyakorta alkalmazzák az olcsóbb rendszerekben az egyszerűbbnek számító DES-t.

4 Data Encryption Standard
Szimmetrikus kulcsú kódolás. Manapság a DES megerősítését, a 3DES-t alkalmazzák, mely a DES kódolás végrehajtása 3-szor egymásután. Tehát az (X=1…3)DES sorra 64, 128 és 192 bites kulcsokat alkalmaz.

5 Advanced Encryption Standard
Hivatalosan az USA Szabványügyi és Technológiai Intézete (National Institute of Standardisation and Technology) fogadta el 2001-ben, és váltotta le az elavultnak számító DES-t. Azonban továbbra is gyakorta alkalmazzák az olcsóbb rendszerekben az egyszerűbbnek számító DES-t.

megjegyezni, hogy a Mifare Classic kártya nem smart card, tehát nem rendelkezik önálló mikroprocesszorral, hanem csak egy memóriakártya.) A feltöréseket legnagyobb számban e kártyák ellen hajtották végbe, mivel a szabványokban nem határozzák meg a szükséges védelmi szinteket, vagy akár a kölcsönös hitelesítést ezen olcsó kártyákra vonatkozóan. *(Pl. a Calypso tömegközlekedési nyílt szabványban alkalmazott kártyák ugyan drágábbak, de hibatűrőbbek, megtalálható a kölcsönös hitelesítés az alkalmazott kártya intelligenciája miatt, továbbá feltörés védettebb a rendszer is.)*

3. KOMMUNIKÁCIÓ

Először ismerjük meg az alkalmazott szabvány *(ISO/IEC 14443 [6]A típus)* a kártyára és az olvasóra vonatkozó főbb jellemzőket.

Olvasótól a kártya felé irányuló kommunikáció jellemzői a következők:

100%-os ASK modulációt használ, módosított Miller [7]kóddal. A kommunikáció sebessége 106 kbit/sec. A modulációs impulzusok szélesség 2,28µs, ez lehetővé teszi a passzív[8] kártya energiával való ellátását.

A kártyától az olvasó felé irányuló kommunikáció jellemzői:

Manchester-kódolást[9] alkalmaznak a bitek megkülönböztetéséhez. 847,5Khz-es vivőfrekvenciával. *(Egész számú többszöröse a kommunikációra használt 13,567Mhz-es frekvenciának.)* Az adatokat a kártya az olvasó erőterébe kerülve ellenállásuk megváltoztatásával *(Az olvasó és a kártya tekercsantennája között induktív kapcsolat áll fent. Ennek folytán a kártyába beépített terhelő ellenállás az olvasóban feszültségesést okoz. Melyet, ha ki-bekapcsolgatunk, akkor feszültségingadozás keletkezik. Az ellenállás ki-bekapcsolás pedig az adatoknak megfelelően történik. Pl.: Bináris 0: 0V, bináris 1: 5V.)* küldenek adatokat.

Egy bit átviteléhez 9,44µs-ra van szükség. A passzív kártyák simítókondenzátorokat is tartalmaznak, hogy kisimítsák a tápellátásban lévő ingadozásokat. A kártya alapállapotban *IDLE (tétlen)* állapotban van. Az olvasó periodikusan küld egy *REQA (Request Type A)* parancsot, ami a hatósugarában lévő összes kártyát *READY* állapotba teszi, gyakorlatilag kész állapotba teszi. Aztán a kártya (kártyák) küldenek egy *ATQA (Amswer to Request Type A)* parancsot, ezzel az olvasó tudja, hogy legalább egy kártya van a hatósugarában. Ha több kártya van az olvasó hatókörében, akkor a 14443 A típusra jellemző „bináris kereső fa” *(binary search tree)* algoritmust használj a kártya kiválasztására. Az olvasó küld egy *SELECT (kiválasztás)* parancsot egy *NVB (Number of Valid Bits- Érvényes Bitek Száma)* paraméterrel és egy bitmaszkot. A maszkban lévő bitek száma az *NVB*-től függ. Majd ez a maszk összekomparálódik a kártya saját ID-jével *(ID=Identification Number)*. Ez a komparálás addig ismétlődik, míg egy kártya kiválasztásra nem kerül *(Legalább 64 db érvényes bitnek*

---

[6] ISO/IEC 14443-2: modulációs eljárásra, és kódolásra vonatkozó sémák.
ISO/IEC 14443-3: ütközés elkerülésre *(anti collison)* vonatkozó sémák.
ISO/IEC 14443-4: kommunikációs protokoll leírása.

[7] A Módosított Miller kódolás, vagy más néven Módosított Frekvenciamodulált kódolás a Frekvenciamodulált eljáráson alapszik. A *függelékben található II. ábrán* látható, hogy az FM kódolás minden bitkezdetre és végre betesz egy kezdő és záró impulzust. Ha 0-lát akarunk kódolni, akkor a cella középen üresen marad, ha 1-gyet, akkor nem. A módosított változat *(az ábrán: MFM jelöléssel)* csak annyiban különbözik, hogy elhagyjuk a kezdő és végimpulzusokat.

[8] 3 típus létezik az RFID kártyákból: passzív, szemi-passzív *(semi-passive)* és aktív. A passzív kártyákat az olvasó készülék látja el a kommunikációhoz szükséges energiával. Az aktív kártyák saját áramforrással *(beépített elem)* rendelkeznek, ennek hatására az olvasási távolság a több métert is elérheti. A szemi-passzív kártya működtetése saját áramforrásból származik, kommunikációhoz viszont az olvasó erőterét használja.

[9] Az informatikai rendszerekben ritkán alkalmaznak bináris kódolást, mivel a vevő nem tudja megállapítani, hogy hol vannak a bitkezdetek és a bitvégek. Ehelyett a függelékben található III. *ábrán* látható Manchester-kódolás a használatos. A bináris 1 a bitcella első felében magas, a 0 pedig a második felében magas.

kell lennie!) Ezután a kártya visszatér egy *SAK (Secure Attention Key)* paranccsal és *ACTIVE* állapotba kerül. Ezek után az olvasó és a kártya lebonyolítja egymás között – a megfelelő protokoll szerint – az adatcserét a következő módon: az olvasó először küld egy *RATS (Request Answer to Select)* parancsot, erre válaszul a kártya visszatér egy *ATS (Answer to Select)* paranccsal, ami már tartalmazza a kártya beállításait.
A teljesség kedvéért fontos megemlíteni, hogy az adatkapcsolati réteg kommunikációs protokollja az ISO/IEC 7816-3 T=1 protokollján *(Fél-duplex aszinkron átvitel)* alapul.

3.1. A személyes adatokról

Ha valahol valamilyen ok miatt szükséges adataink egy rendszerben való rögzítése, akkor mindig felmerül az a kérdés, hogy vajon biztonságban vannak-e az adataink, lehetséges-e külső, vagy akár belső személy általi visszaélés? Adataink védelméért, illetve biztonságát az *2011. évi CXII. törvény* szabályozza. Mely hazánkban a többi európai ország adatvédelmi törvényéhez képest nagyobb szigorral szabályoz. A legtöbb kártyán letárolásra kerülnek a személyes adatok. Hazánkban a megszemélyesítés a személyes adatok direkt rögzítésével egy kártya adathordozóján, az adatvédelmi törvény miatt még nem megoldható. Azonban pl. egy ráragasztott matricával már kikerülhető ez a probléma.

4. MIFARE KÁRTYÁK FELÉPÍTÉSE

A világ túlnyomó részén az NXP Mifare kártyákat alkalmazzák. *(Hozzávetőlegesen az összes RFID média 70%-kát fedi le.)* A bérletre leggyakrabban használatos kártya a Mifare Classic 1K és 4K. *(A nem megfelelő biztonság miatt a Classic 1K kártyák Angliában 2016.12.31-ig fokozatosan kivonásra kerülnek.)* A Classic kártyák egy EEPROM-ot és egy rádiófrekvenciás kommunikációt lehetővé tevő interfészt tartalmaznak.

EEPROM felépítése:

MIfare Classic 1K-nál 16db 64 byte-s szektor található, és minden szektor tovább bonható 4db 16 byte-s blokkra. *(Tehát összesen 64 db blokk található egy 1K-s EEPROM-ban.)* Minden szektor utolsó blokkja a tartalmazza a „trailer” részt, mely 2 titkos kulcsot és programozási hozzáféréseket tárol. A függelékben található *I. ábrán* látható a felépítése.

Szektor	Blokk	0 1 2 3 4 5	6 7 8 9	10 11 12 13 14 15	Leírás
15	3	KEY A	ACCESS BITS	KEY B	TRAILER SZEKTOR 15
	2				DATA
	1				DATA
	0				DATA
14	3	KEY A	ACCESS BITS	KEY B	TRAILER SZEKTOR 14
	2				DATA
	1				DATA
	0				DATA
1	3	KEY A	ACCESS BITS	KEY B	TRAILER SZEKTOR 1
	2				DATA
	1				DATA
	0				DATA
0	3	KEY A	ACCESS BITS	KEY B	TRAILER SZEKTOR 0
	2				DATA
	1				DATA
	0				MANUFACTORER BLOCK

1. ábra. Mifare Classic 1K logikai felépítése
Forrás: http://www.cardviser.hu/muszaki_ismerteto.php?id=58; (2011. 03. 14.)

5. TÁMADÁSI MÓDSZEREK

A Mifare kártyák ellen sokféle támadás létezik. A támadások lényege, hogy az adatkapcsolati réteg számára teljesen láthatatlan, mivel a támadások a fizikai rétegre irányulnak.

Az egyik módszer a *lehallgatás*. Egy az erre készített céleszközzel lehallgathatjuk a kártya és az olvasó közötti kommunikációt. Majd pl. az igazi kártya eltulajdonítása után lehetséges az adatok teljes visszafejtése a lehallgatott kommunikációs adatok segítségével.

A következő módszer a *klónozás*, ez akkor jelent gyakorlati problémát, amikor a kártya nincs védve semmiféle titkosítással, továbbá ismert a kártya utasításkészlete. Védelem nélküli, olcsóbb kártyáknál kivitelezhető. Továbbá a klónozás egyszerűen kivédhető a duplikált kártyák figyelésével.

A harmadik módszer az eldobható RFID kártyáknál jelentkezhet, melynél a risszul tervezett rendszer nem figyeli a Lock bit-ek letiltását. Ezzel lehetővé teszi a kártya memóriaterületére való írást. Ezzel pl. jogtalanul újra felhasználhatunk egy kártyát.

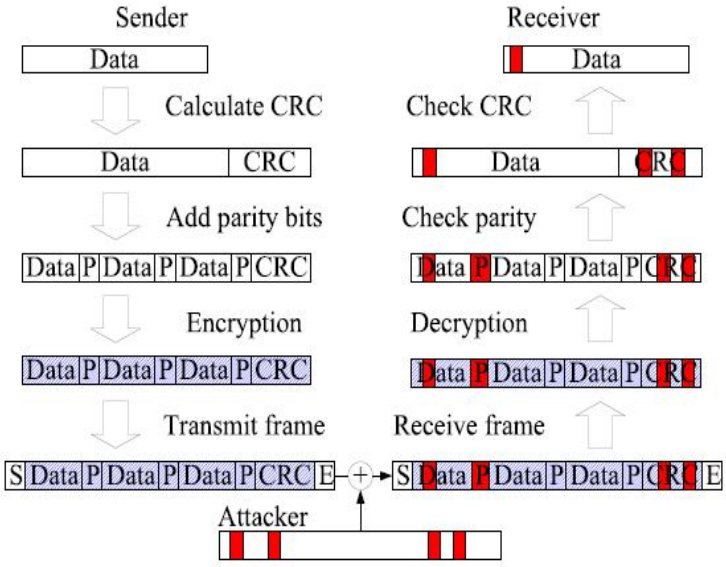
A negyedik megoldás egy hardware-es törési lehetőség a *reverse engineering*. Ha eltulajdonítottunk egy kártyát, és a tervezők nem figyelnek a kártya hardware-es védelmére, akkor visszafejthető a chip hardware-es felépítése, utasításkészlete, stb.

Végül a legveszélyesebbnek vélt módszer a *man in the middle (ember a középpontban, vagy ismertebb nevén közbeékelődéses támadás),* amelyen belül két változatot is meg tudunk különböztetni: az aktív és a passzív módszer. Az aktív módszerrel az áldozat kártyáján változtatásokat is végzünk, passzívnál nem. Talán ehhez a törési formához kell a legkisebb anyagi befektetetés *(100 angol fontból kihozható céleszközt készítettek már 2005-ben)*, és az, hogy a támadó hogyan vitelezi ki csak a kreativitásától, és szakmai ismereteitől függ. A lehallgatástól annyiban tér el, hogy a lehallgatott anyag azonnal felhasználásra kerül. Ehhez két célszerkezet szükséges: egy eredeti kártyaolvasó *(Pl. egy nyílt forráskódú OpenPCD olvasó.)*, és egy Ghost kártyát *(Ez egy eredeti RFID kártya, azzal a különbséggel, hogy számítógéphez csatlakoztatható és programozható.)*. A Ghost kártya az eredeti terminállal felveszi a kapcsolatot, majd továbbítja a terminál által küldött parancsokat a számítógépnek. A számítógép a parancsokat továbbítja az OpenPCD-nek, majd az OpenPCD az eredeti kártyának. Majd visszafelé is lefolytatódik ez a kommunikáció. Az olvasó és a terminál gyakorlatilag azt érzékeli, hogy egymással kommunikálnak, és nincs „középen senki”. Ráadásul nem érdekli a támadót, hogy DES vagy AES kódolással titkosították a kártyát, hiszen megvan számunkra minden kellő információ. Tehát ezzel gyakorlatilag megszereztünk minden adatot, ahhoz hogy egy kis időre „kölcsön vegyük” az áldozat kártyáját. Ez egy bérletnél nem is lenne gond, de ahol a bérlet funkció mellett elektronikus pénztárca funkció is megtalálható, és ezen az elektronikus számlán pénz is található, akkor komoly bevétele lehet a támadónak egy ilyen támadás lefolytatása után. Végezetül az áldozat semmit sem vesz észre a támadás alatt.

Azt fontos megjegyezni, hogy egy átlagos kártya maximális leolvasási távolsága nem haladja meg az 1cm-t az alkalmazott kis hatótávolságú antennája miatt. Ezt azzal ki lehet küszöbölni, hogy létrehozunk egy loop antennát, melyet akár egy teniszütőnek is lehet alkalmazni, oly módon hogy a loop antennával teniszütőformát alakítunk ki, és betesszük egy teniszütő tokba. *(Fontos, hogy a terminállal kommunikáló céleszköznek közel kell lennie az olvasó terminálhoz.)* Visszatérve a loop antennára, segítségével az átjátszási távolság a többi eszköz felé akár 50m-ig is könnyedén kitolható. A lényeg, hogy rövid ideig folyamatos kapcsoltban legyünk a támadott kártyájával.

Többféle kivitelezési mód is létezhet. Az egyik módszer, az esetleges csaló kereskedőkön alapszik. Pl. ha egy kereskedő elhelyez egy hamis kártya feltöltő állomást az üzleténél, akkor plusz bevétele szárazhat abból, hogy a csaló automata csak szelektíven továbbítja a bevételről

szóló adatokat tömegközlekedési társaságnak. A másik, ezen alapuló módszer az, hogy egy szintén csaló kereskedő rejtve elhelyez egy kicsi loop antennát a terminál kártyaolvasójához közel. Kiszemel egy áldozatot, aki frissen töltötte fel a kártyáját, és belépéskor a kereskedő képes megtámadni az áldozat kártyáját, és lecsípni belőle valamekkora összeget. A dupla transzakció *(a törvényes belépésért, és a csalásért)* időben nem észrevehető. A nem túl nagy lecsípett összeg pedig általában nem tűnik fel senkinek. Ez ellen a kártyafeltöltők és a beléptető terminálok együttes figyelhetősége lenne a megfelelő ellenszer. A második módszer azon alapszik, hogy van egy éves bérletünk, és a rendszer nem figyeli a duplikátumokat. Ha csak helyileg figyeli a duplikátumokat, akkor a klónkártyákat felhasználóknak más útvonalon kell közlekedniük. A korábban írottak szerint itt le kell figyelni a rádiófrekvenciás kommunikációt a kártya és a terminál között. Az adatokat felhasználva, pedig létrehozhatunk több virtuális klónkártyát. A kártyákat szét lehet osztani az ismerősök között, azzal a megkötéssel, hogy senki ne menjen ugyanazon a kapun be. Végül a harmadik módszer a Mifare Classic nem megfelelő hitelesítésen, illetve titkosításon alapszik. A man in the middle módszerrel a támadó saját kártyájára több pénzt tölthet fel, mint amennyit befizetett az automatába. A lényeg az, ami a *2. ábrán* is látható, hogy a támadó céleszközökkel bele képes nyúlni a feltöltő terminál által küldött adatkeretbe, azzal meghamisítva a kártya által vett adatkeretet. Természetesen ennél több lehetőség is nyílhat a támadó számára, és nem csak a tömegközlekedés nyújtotta területeken.



2. ábra [1]

E technikák ellen a distance bounding protokoll (távolság korlátozás) használata, illetve a time relay figyelése adhat megfelelő védelmet. (time relay= késés Egy végrehajtott támadás kb 20µs-os késleltetést vitt be a rendszerbe. Csak hasonlításképpen a Frame Waitng Time, azaz a megengedett időtúllépés az ISO/IEC 14443-4 szerint ez FWT=300-tól 5s-ig változhat.) További megoldás lehet egy ultrahangos érzékelő elhelyezése, mely egy beállított távolságlimit után megszakítja a kommunikációt és jelez. A működés azon alapszik, hogy a hangsebesség alacsonyabb a fénysebességnél. Az eszközök Faraday kalickába zárása is megoldást nyújthat a káros rádiófrekvenciás lehallgatások ellen.

6. ÖSSZEGZÉS

Napjainkban a bűnözés nagy része áttevődött a virtuális világba, tehát a"tudós" bűnözők nagy része nem az utcán, szemtől szembe támad a kiszemelt áldozatra, hanem azt a modern információs technológiának köszönhetően a virtuális téren keresztül teszi. Az emberi tehetséget rosszra felhasználók sajnálatos módon már a nagybiztonságú, nyílt forráskódú memóriakártyák feltörésére is képesek lehetnek. Szerencsére a másik oldalon is léteznek leleményes szakemberek, akik azon dolgoznak, hogy optimális védelmet építsenek ki a bűnözők ellen. Erre jó példa a mikroprocesszorral rendelkező intelligens kártya, a smart card, melynek ismertetése egy másik cikk témája lehet.

Felhasznált irodalom

[1] G.P. Hanckea, K.E. Mayesa, K. Markantonakisa, Confidence in Smart: Token Proximity: Relay Attacks Revisited, ISG Smart Card Centre Royal Holloway, University of London Egham TW20 0EX, UK, 2009

[2] Wouter Teepe: Making the Best of Mifare Classic Update, Raunbunk University Nijmegen, 2008

[3] Gerhard de Koning Gans, Jaap-Henk Hoepman, and Flavio D. Garcia: A Practical Attack on the MIFARE Classic, Institute for Computing and Information Sciences, Radboud University Nijmegen, 2008

[4] Gerhard Hancke: A Practical Relay Attack on ISO 14443 Proximity Cards, University of Cambridge, Computer Laboratory JJ Thomson Avenue, Cambridge, CB3 0FD, UK, 2005

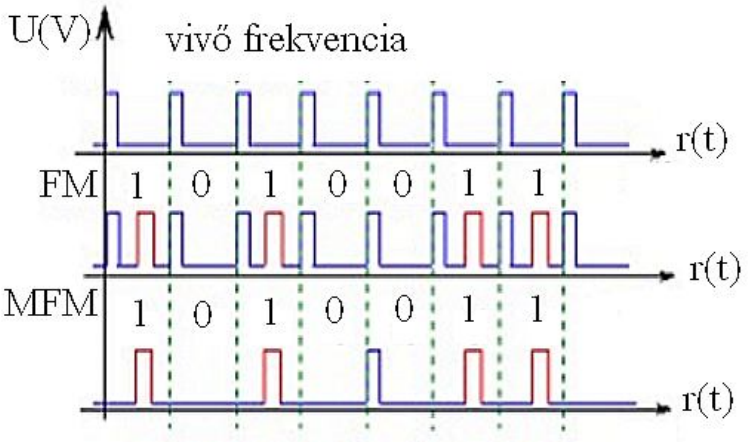
[5] ISO/IEC 14443-4:2008 Identification cards -- Contactless integrated circuit cards -- Proximity cards -- Part 4: Transmission protocol, 2008.06.04.

[6] ISO/IEC 7816-1:2011 Identification cards -- Integrated circuit cards -- Part 1: Cards with contacts -- Physical characteristics, 2011.01.31.

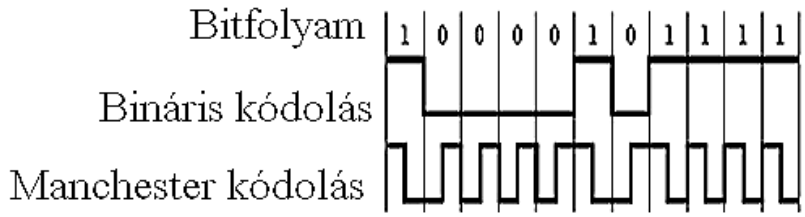
[7] i.sz.: http://vili.pmmf.hu/jegyzet/diplom/1997/lauko/kodok.htm; (2011. 09. 13.)

[8] i.sz.: http://www.remenyikzs.sulinet.hu/segedlet/addatar/adattar.html; (2011. 03. 14.)

Függelék



I. ábra. FM és MFM kódolás [1]



II. ábra. Manchester kódolás
Forrás: http://vili.pmmf.hu/jegyzet/diplom/1997/lauko/kodok.htm; (2011. 09. 13.)