Alkalmazott Matematikai Lapok **23** (2006), 389–403.

KRIPTOGRÁFIAI KULCSVISSZAÁLLÍTÓ RENDSZEREK

PAPP PÁL

A kriptográfiai biztonság egyik alapeleme, hogy a véletlenszerűen választott üzenetkulcsot illetékteleneknek ne lehessen visszaállítani, megfejteni. Maguknak a felhasználóknak, vagy a törvény alkalmazóinak azonban szükségük lehet arra, hogy a rendelkezésre nem álló kulcsot rekonstruálják. Jelen dolgozatban ennek az ellentmondónak látszó feladatnak a megoldására kidolgozott eljárásokat ismertetjük, felvillantva a mögöttük rejlő matematikai ismereteket. A cikk második részében egy konkrét feladat kapcsán áttekintjük a felmerülő gyakorlati problémákat, és egy új, szimmetrikus kriptográfián alapuló megoldást mutatunk be egy részproblémára.

1. Bevezetés

Digitális üzenetek, dokumentumok biztonságának, hozzáférhetetlenségének egyik legfőbb eszköze egyértelműen dekódolható kódok alkalmazása. Az eljáráshoz lerögzítik kódoknak egy paraméteres halmazát, és a rejtjelzés ezek egyikének alkalmazásából áll. Az aktuális kód paraméterét véletlenszerűen választják az összes lehetséges paraméter közül. A kiválasztott paraméter értékét kulcsnak nevezik. A dekódoláshoz ezt a kulcsot kell ismerni, ennek ismeretében a dekódolás gyorsan végrehajtható művelet, ismeretének hiányában történő fejtés (rejtjelfejtés) viszont gyakorlatilag kivihetetlen. A kulcsok biztonságos kezelése adja meg az elvárható biztonságot.

Mind a hírközlés, mind az adattárolás esetében alapvető biztonsági rendszabály, hogy a rejtjelzett dokumentumokat és a rejtjelezésükhöz használt kulcsokat szigorúan elkülönítik egymástól. Így előállhat az a helyzet, hogy a kulcs(-hordozó) megsemmisül, míg a rejtjelezett dokumentum épségben megmarad. Természetesen merül fel tehát az igény arra, hogy ilyen esetekben is vissza lehessen állítani az eredeti nyílt szöveget. Mivel ez a kulcs nélkül az adatbiztonság alapvető követelménye

miatt gyakorlatilag lehetetlen, így az egyetlen megoldás olyan kulcsrendszer tervezését, alkalmazását jelenti, amelyben a legális felhasználó képes a kulcsot visszaállítani. A dolgozat címe ezt az igényt tükrözi, ennek a feladatnak a megoldására összpontosít.

Feladatunk nem merő fantázia kérdése. Az elmúlt néhány évben gyakorlatunkban több esetben fordult elő, hogy a kulcs megsemmisült. Találkoztunk olyan esetekkel is, amikor egy cég számítástechnikai alkalmazottai összehangolt zsarolást alkalmaztak a cég vezetőségével szemben: a teljes adatállományt lerejtjelezték, majd a visszaállításhoz szükséges kulcs kiadását sok milliós „váltságdíj" kifizetéséhez kötötték. Ezekben az esetekben magánszemély, vagy vállalat érdeke volt a kulcs visszaállítása. (A konkrét eseteinkben a kriptográfiai rendszer hibás megtervezése miatt ez gyorsan megtörténhetett.)

Van egy harmadik terület, ahol a kulcsvisszaállítás igénye országos jelentőségű. Jogi, ítélkezési, biztonsági követelmények kielégítése szükségessé teheti, hogy a kulcsot birtokló entitás hozzájárulása nélkül is elérhető legyen a kriptográfiai operáció által védett nyílt szöveg. Ezen a területen emlékezetes az akkoriban nagy felzúdulást váltott ki az USA kormányzatának Clipper chip projektje (1993). (1. Függelék)

Egy ilyen rendszer célkitűzése az, hogy a rejtjelzéssel védett kommunikációt éppúgy lehallgathatóvá tegye az államhatalom számára a megfelelő engedélyek birtokában, mint a nyílt kommunikációt. Ilyen rendszer tervezésénél több, ma megoldhatatlannak látszó matematikai és hírközlési probléma is jelentkezik. Problémát jelent a lehallgatható kommunikációs rendszer kikerülhetetlenségének biztosítása, a szükséges rendszer hatalmas mérete éppúgy, mint az emberi jogok betartásának biztosítására adandó, informatikai jellegű garanciák beépítése.

A kulcs esetleges, speciális helyzetben megtehető visszaállíthatósága természetes igényként jelentkezik az üzemeltető részéről a kriptográfiai rendszer működtetése során. Távolabbról nézve, vagy a rendszer biztonságáért felelősséget viselő pozícióból pedig minden ilyen igény ésszerűtlen, és bármilyen, ezt a célt szolgáló megoldás aláássa a rendszer biztonságát. A kompromisszumos megoldás szükségessége akkor válik nyilvánvalóvá, amikor kulcsvisszaállító rendszer működtetése nélkül az egyéni felhasználó a végleges adatvesztés miatti félelmében inkább nem is használja a kriptográfiát, illetve az államhatalom csak általa kezelhető erősségű kriptográfiai megoldásokat engedélyez azért, hogy szükség esetén gyakorolni tudja az információhoz való hozzáférésének jogát.

A kulcsvisszaállítás többféle célokat szolgálhat, s ennek megfelelően az alkalmazandó módszerek is jelentősen különböznek. Mi a három nagy részterületnek megfelelően foglaljuk össze őket. Az általános esetek felvázolás után egy konkrét gyakorlati problémát és annak megoldására kidolgozott módszerünket ismertetjük.

2. Kulcsvisszaállító rendszerek állami környezetben

Elvi szintű problémát jelent az a meggondolás, hogy míg a rendszer alapcélja a bűnözők lehallgatása, a társadalmat érő fenyegetések csökkentése, addig maga a kulcsvisszaállító rendszer visz be új támadási lehetőségeket az informatikai rendszerbe. A problémára adott legismertebb elvi szintű válasz S. Micali rendszere. (2. Függelék)

Magyarországon nem érzékelhetőek törekvések kulcsvisszaállító rendszer felállítására. Annyira nem, hogy a legutóbbi időkig a polgári szféra híján volt mindennemű informatika biztonsági jellegű hatóságnak. Ez a 2001-ben elfogadott Elektronikus aláírás törvénnyel részben megváltozott, mert a törvény hatósági, felügyeleti jogokat adott a Hírközlési Felügyeletnek (ma már Nemzeti Hírközlési Hatóság) az elektronikus aláírás termékekkel kapcsolatban.

A távközlési vonalak lehallgatása érzékeny kérdés hazánkban is. A lehallgatást minden esetben az igazságügyminiszter engedélyezheti, korlátozott időre. A törvény célja, hogy közvetlen politikai kontroll legyen a lehallgatást igénylő szervezetek (rendőrség, nemzetbiztonsági szolgálatok, pénzügyőrség, stb.) fölött.

3. Kulcsvisszaállító rendszer vállalati környezetben

A kulcsvisszaállító rendszerek alkalmazásának optimális területe a vállalati szféra, abban az értelemben, hogy ebben a nagyságrendben a feladat gyakorlati szempontból jól kezelhető, az irányítás egységes, centralizált, a rendszer elemei azonos biztonságpolitika alatt működnek. Ebben a körben is jelentős az igény ilyen megoldásokra. Ennek oka az, hogy a vállalati rendszerekben kezelt adatok nyilván a vállalat tulajdonát képezik, ezek az adatok fontosak, esetleg kritikusak lehetnek a cég működtetése szempontjából. Ezért biztosítani kell azt, hogy a cég akkor is hozzá tudjon férni a védett adatokhoz, ha a kulcsot birtokló alkalmazott ebben nem tud, vagy nem akar közreműködni. Ennek több oka lehet a kulcshordozó elvesztésétől kezdve egy véletlen balesetig. A továbbiakban a vállalati környezetben szükséges megoldásokat vizsgáljuk, bár sok részmegállapítás szinte változatlan formában igaz a másik két alkalmazási területre is.

A kulcsvisszaállító rendszer megtervezése előtt tisztázni kell, hogy mit várunk el a rendszertől, hogyan kapcsolódik az informatikai rendszer egyéb elemeihez, és azt is, hogy az informatikai rendszernek milyen segítséget kell adni a kulcsvisszaállító rendszer hatékony működéséhez.

Fontos eldöntendő kérdés, hogy milyen adatok visszaállítására van/lehet szükség. Nyilvánvaló, hogy még a kulcsvisszaállító rendszer segítségével is csak olyan adatok állíthatók vissza, amelyek később, amikor a visszaállítás szükségessé válik, legalább rejtjelzett formában hozzáférhetőek. Ez általában nincs így a rejtjelzéssel védett kommunikációs vonalak esetében.

Ha igényként merül föl a védett kommunikáció visszaállítása, akkor az különleges feladatokat ró a kulcsvisszaállító rendszerre. A legtöbb kommunikációs protokoll esetében az aktuálisan használt kapcsolati kulcs mindkét fél kulcsától függ, vagyis a visszaállításhoz mindkét fél kulcsára szükség van. Emellett a kulcsvisszaállító rendszernek képesnek kell lennie szimulálni azt a módszert, amivel a protokoll a két kommunikáló fél kulcsából az aktuális kommunikációs kulcsot előállítja. Ez sokszor, pl. a leggyakrabban használt TLS/SSL protokoll esetén meglehetősen bonyolult. A kulcskialakítás módja attól is függhet, hogy a két fél között az első kapcsolat jön létre, vagy már a sokadik.

Vállalati környezetben védett kommunikáció visszaállítása ritkán merül fel igényként, ez inkább a kormányzati szintű rendszerekre jellemző. A vállalati környezetre a tárolt adatok és az e-mail forgalom visszaállításának az igénye a jellemző.

A feladat konkrét technikai megoldása során általában két megoldási módot szokás követni. Az egyik esetben az aktuális rejtjelző kulcsot egy Megbízható Kívülálló (TTP = Trusted Third Party) nyilvános kulcsával is rejtjelezzük, és a kulcs rejtjeles képét együtt kezeljük (tároljuk, továbbítjuk) a rejtjelzett anyaggal. Így a rejtjelzett anyag mellett mindig rendelkezésre áll a rejtjelzéséhez használt kulcs, igaz, csak a TTP által elérhető, rejtjelzett formában. Ezt a megközelítést alkalmazza többek között a hazánkban általánosan alkalmazott PGP (Pretty Good Privacy, „tök jó biztonság") eljárás is. Ebben a TTP kulcsát Additional Decryption Key (= ADK, „kiegészítő megoldó kulcs)-nek nevezik. A megoldás hátránya, hogy a TTP privát kulcsának kompromittálódása minden, korábban végzett rejtjelzést veszélyeztet, ezért ezt kiemelten kell védeni. A megoldás tökéletes lehet egy magánszemély számára, azonban vállalati környezetben nem megfelelő.

A rendszer elterjedésénél a legkomolyabb problémát az okozza, hogy nincs ipari szabvány ezen a területen. Ez a technika a korábban készült alkalmazásokba utólagosan gyakorlatilag már nem építhető be. A korábban készült rendszerek fejlesztői sokszor nem elérhetők, a módosítást jogi problémák akadályozhatják, esetleg túl költséges ez a megoldás. Elmondhatjuk, hogy ezen a módon egységes, minden érintett applikációt lefedő kulcsvisszaállító rendszer gyakorlatilag nem építhető ki.

A nyilvános kulcsú kriptográfiai rendszerekben a másik gyakori megközelítési mód az, hogy a felhasználók titkos kulcsait tárolja le a TTP megfelelő védelem mellett. (Emlékeztetünk arra, hogy ezekben a rendszerekben a felhasználók két kulcsot használnak, egy nyilvános kulcsot, amelyet „telefonkönyv-szerűen" nyilvánosságra hoznak, és egy titkos kulcsot, amelyet a legszigorúbban őriznek. Egy megbízható harmadik fél, u.n. „hitelesítésszolgáltató" tanúsítja, igazolja, hogy a nyilvános kulcsot valóban az helyezte el, akinek vallja magát.) A védelem egyik eleme az, hogy a titkos kulcsot több TTP között osztják meg. Ehhez legtöbbször a Shamir–Blakley (függelék) sémát használják.

Ez a megközelítési mód akkor lehet hatásos, ha a cégen belül a kriptográfiai alkalmazások kulcsellátására egységes, centrális rendszert alkalmaznak. A gyakorlatban a kulcsvisszaállító rendszert célszerű a vállalati hitelesítés-szolgáltatási rendszerhez kapcsolni.

4. Kulcsvisszaállító rendszer egyéni használatra

Az alkalmazási spektrum másik végén az az igény áll, hogy egy egyedi felhasználó is legyen képes visszaállítani rejtjelzett fájljainak tartalmát, ha a kulcs hordozója elveszett, megsérült, vagy a felhasználó elfelejtette a kulcs védelméhez használt jelszót. A megjelenő igény valós, ugyanis a kriptográfiai védelem elterjedésének egyik legnagyobb gátja éppen az, hogy a megfelelően rejtjelzett adat gyakorlatilag senki által semmilyen módon nem helyreállítható a kulcs nélkül, s ettől a felhasználók idegenkednek. Megszokták, hogy a papíralapú kommunikációnál, de még a számítógépes adattárolás esetén is mindig van, marad esély az adatok visszaállítására. Ennél a megközelítésnél a problémát az okozza, hogy vagy bevonunk külső szereplőket a felhasználó mellé, aki, vagy aki segítségével a felhasználó vissza tudja állítani a védett adatokat, vagy csupán annyit teszünk, hogy a felhasználó környezetében a visszaállításhoz szükséges állományokat megtöbbszörözzük. Az első megközelítés új szereplőt hoz a színre, ezért hátrányos, míg a második megközelítésben ismét minden a felhasználóra van bízva, még ha a kulcselvesztés valószínűségét csökkentjük is.

5. Egy konkrét gyakorlati probléma

A cikk további részében egy konkrét feladat kapcsán esettanulmány jelleggel szeretnénk ismertetni egy nagyméretű, jelentős informatikai potenciált használó cég esetében felmerült meggondolásokat, illetve az ott alkalmazott egyedi megoldást. A cég már eddig is jelentős, részben központosított infrastruktúráját kulcsvisszaállítási képességekkel kívánta kiegészíteni. Az informatikai rendszerben több különböző korú, és különböző forrásból származó kriptográfiai képességekkel rendelkező szoftvert használnak, ezért az Additional Decryption Key-re épülő módszereket ki kellett zárni. Az alkalmazott informatikai rendszerben a rejtjelzéssel kapcsolatban felmerült igények meglehetősen tipikusak. Szükség van:

- Titkosított e-mail forgalomra,
- Rejtjelzésel védett lokális adattárolásra,
- Adatbázisrekordok védett tárolására, ezek távoli elérésére,
- Kommunikációs kapcsolatok rejtjelezéssel történő védelmére (TSL, SSH, különböző, főként IPSEC alapú VPN megoldásokra,
- A rendszerben egy belső hitelesítésszolgáltató biztosítsa a nyilvános kulcsú infrastruktúra alapjait, amelyhez saját fejlesztésű RSA kulcsgenerátor is csatlakozzon, így garantálva a kulcsgenerálás biztonságát, átláthatóságát, auditálhatóságát.

Fontos eleme a biztonsági környezetnek, hogy a felhasználók titkos kulcsai modern, a legfrissebb támadási módszerek ellen (Differential Power Analysis, Fault Analysis) is megbízható smart cardra kerülnek. A rendszer rendelkezik olyan védett adatközponttal, amely megbízható fizikai védelmet adhat egy olyan kulcsnak,

amelynek megismerése a teljes informatikai rendszer biztonságára kihat. Ilyen kulcs a PKI Hitelesítés Szolgáltató mester kulcsa, de egy bevezetendő kulcsvisszaállító rendszer is egy ilyen, kiemelt védelmet igénylő kulcsot visz a rendszerbe. Rendelkezésre áll olyan szervezeti egység is, amely alkalmas lehet a Megbízható Kívülálló (Trusted Third Party) szerepére is. Az adatközpont kulcsainak védelme a teljes rendszer szempontjából rendkívül fontos, ezért ennek védelmét kiemelt fizikai biztonsági és rezsim intézkedésekkel kell biztosítani.

A kulcsok generálása központilag történik, vagyis lehetőség van arra, hogy egy kulcsvisszaállító rendszer a központban működve, a központi kulcsgenerálásra alapozva tegye lehetővé az egyedi felhasználói kulcsok elérését.

Mivel a rendszer smart cardokat alkalmaz kulcshordozóként, a kulcsok generálásának kézenfekvő módja a smart card kulcsgeneráló funkciójának használata, amely azt is lehetővé teszi, hogy a generált kulcs ne legyen kiolvasható, kívülről elérhető, csak a kártya operációs rendszere számára legyen látható. Ez a megoldás, bár jelentősen növeli a biztonságot, csökkenti a szervezési feladatokat és növeli a felhasználók rendszerbe vetett bizalmát, megakadályozza, hogy a kulcsvisszaállító rendszer hozzáférjen a generált kulcsokhoz.

Ugyanakkor a kártyán generált kulcsok optimálisak a digitális aláíráshoz használt kulcsok esetében, sőt a gyakorlatban ez az egyetlen módszer, amely a digitális aláírás letagadhatatlanságát biztosítani tudja. (A kártyán kívül más entitás nem ismeri, nem kerül kapcsolatba a felhasználó digitális aláírásra használt titkos kulcsával).

Ma már elfogadott szakmai tény, hogy nem célszerű digitális aláírásra és rejtjelzésre ugyanazt a kulcsot használni. Ezt az álláspontot képviseli a jelenleg érvényben levő elektronikus aláírás-törvény is. A kétféle kulcsnak más az életciklusa, szerepe, mások az esetleges visszavonás körülményei, mások a kompromittálódás kockázatai. Ezért a megoldás lényege az, hogy míg a digitális aláíráshoz használt kulcsok a kártyán generálódnak, addig a rejtjelzésre használt kulcsokat egy külső, a Hitelesítés Szolgáltató rendszer részeként működő modul generálja, és így lehetővé válik az is, hogy egy kulcsvisszaállító rendszer hozzáférjen a generált kulcsokhoz mielőtt azok a kártyára felírásra kerülnek.

6. A javasolt megoldás

Az alkalmazandó kulcs-vissszaállító rendszerrel szembeni elvárások az alábbiakban foglalhatók össze:

- Legyen képes a központilag generált, rejtjelzésre használandó kulcsok visszaállítására.
- Legyen képes tárolt rejtjelzett fájlok, illetve adatbázisrekordok visszaállítására a rejtjelzést kezdeményező, illetve végrehajtó felhasználó együttműködése nélkül is.
- Legyen képes a rejtjelzett e-mail forgalom visszaállítására is.

- A rendszer kialakítása olyan legyen, hogy a potenciális felhasználókban bizalmat ébresszen, garanciákat adjon arra, hogy a kulcsvisszaállító rendszer csak indokoltan, megfelelő kontroll mellett kerül felhasználásra.
- A rendszer rendelkezzen olyan kriptográfiai mechanizmusokkal, amelyek a biztonság szubjektív sugalmazása mellett objektíven is védelmet adnak, biztosítják az előző pontban leírt célok megvalósulását.
- A digitális aláíráshoz használt kulcsok visszaállítása nem elvárás.
- Védett kommunikációs kapcsolatok (kivéve e-mail) visszaállítása nem elvárás.

A tervezett megoldás lényege, hogy az RSA kulcsgenerátor által elkészített kulcsot megkapja a kulcsvisszaállító rendszer. A kulcsvisszaállító rendszer a kulcsigénylés alapadatai mellett rejtjelzett formában tárolja az igényelt kulcs titkos részét. A rejtjezés visszaállításához szükséges kulcsot a Shamir séma (ld. függelék) segítségével szétosztjuk a titokbirtokosok között. Ennek az úgynevezett küszöbsémának a lényege az, hogy n kiosztott információdarab, úgynevezett árnyék közül bármely m elegendő a titok visszaállításához úgy, hogy bármely $m-1$ árnyék (a sémától függően gyakorlatilag, vagy elméletileg is bizonyítható módon) semmi információt nem ad a titokra. Az alkalmazott séma *véges test fölötti polinom interpoláción* alapul.

Az adatbázis titkos részének védelmére olyan módszert kell alkalmazni, amely annak ellenére biztosítja a titkos kulcsok védelmét, hogy a rejtjelzéshez szükséges kulcs megjelenik a rendszert futtató számítógép memóriájában, hiszen a folyamatosan keletkező titkos kulcselemeket védeni kell. Dolgozatunkban erre a problémára javasolunk egy szimmetrikus kriptográfián alapuló gyors, hatékony megoldást.

Nyilván nem kivitelezhető az a megoldás, hogy a titokbirtokosoknak minden kulcsrejtjelzés előtt vissza kell állítaniuk az adatbázis védelmét biztosító kulcsot.

Kézenfekvő megoldás, hogy az adatbázis védelmére nyilvános kulcsú megoldást alkalmazzunk, hiszen ekkor az adatbázis védelmét biztosító, az újabban keletkező rekordok rejtjelzését lehetővé tevő kulcsot az operációs rendszerben tarthatjuk, míg a megoldáshoz, a védett felhasználói kulcsok hozzáféréséhez az adatbázisvédő kulcs titkos párja szükséges, amelyet a titokbirtokosok megosztva őriznek.

Mivel azonban a nyilvános kulcsú algoritmusok nagyságrendekkel lassabbak a szimmetrikus algoritmusoknál, felmerül a kérdés, hogy az elvárások teljesíthetők-e szimmetrikus kriptográfiai algoritmus alkalmazásával is.

6.1. A múlt titkosságának megőrzése

Bizonyos kriptográfiai protokolloknak van olyan tulajdonsága, hogy az aktuális kommunikációt védő kulcs kompromittálódása nem segíti a támadót a későbbi védett kapcsolatfelvételek megtámadásában. Ezt a tulajdonságot angolul forward secrecy típusnak nevezik. Tipikus megoldási mód, hogy a rejtjelzéshez szükséges kulcsot a kapcsolat elején hozzák létre, például a Diffie–Hellmann kriptorendszer segítségével. A forward secrecy értékes tulajdonság, mert olcsóbbá, biztonságosabbá teszi a rendszer működését, és a rendszer biztonságának bevizsgálása is könnyebb.

Esetünkben a megoldandó alapprobléma az, hogy az operációs rendszerben jelen levő kulcs ne kompromittálja a korábban rejtjelzett rekordokat, vagyis az aktuális kulcs ismerete ne adjon lehetőséget a korábban rejtjelzett rekordokhoz való hozzájutásra. Szükséges még az is, hogy a rekordok rejtjelzésére használt kulcsok származtathatók legyenek abból a mesterkulcsból, amit a titokmegosztási séma segítségével szétosztottunk a visszaállítással foglalkozó (recovery) adminisztrátorok között.

A forward secrecy mintájára ezt az elvárást a továbbiakban nevezzük backward secrecy-nek.

6.2. Az implementáció részletei

Az implementált megoldás lényege, hogy a megosztott mester-kulcsból (Sharedmasterkey) az első rejtjelzés előtt létrehozzuk az AK0 alapkulcsot. Ehhez egy speciális egyirányú transzformációt használunk. Az alapkulcsból iterációval hozzuk létre az AKi Aktuális Kulcsokat. Az AKi kulcsból minden rekord rejtjelzése után egy egyirányú transzformációval létrehozzuk az aktuális AK($i+1$) kulcsot. Egyirányú transzformációként az USA szabványban szereplő SHA256 hash-függvényt használjuk. Ennek nagyobb outputja csökkenti a rövid sorozatok hash-eléséből következő elvi sebezhetőséget.

Az AKi.kulcsból és az i. rekord névmezőjéből származtatjuk a rejtjelzésére használt ENCRYPTKEYi kulcsot. Az előző kulcsra gyakorlatilag nem lehet visszakövetkeztetni, de mivel természetesen van kapcsolat az AKi kulcsok között, a választott megoldás gyakorlati és nem elméleti szinten ad biztonságot.

A kulcsvisszaállító rendszer egy külön modul, amely inputként a megosztott mesterkulcs visszaállításához szükséges árnyékokat, a visszaállítandó kulcs i. sorszámát és a felhasználó nevét (commonname) kéri be. Az alrendszer outputja az ENCRYPTKEYi, illetve a kapcsolódó kezdővektor. Az ENCRYPTKEYi szerepe az, hogy a kulcsvisszaállítás egyedivé váljék, csak a kérdéses rekord kerüljön visszaállításra. Ha közvetlenül az AKi kulcsot használnánk rejtjelzésre, akkor nemcsak az i. rekord, hanem minden utána következő is visszaállíthatóvá válna.

A kulcsadatbázis létrehozása során egy rekordjának szerkezete a következő típusú lesz:

A kulcsbirtokos azonosítói

- i, azaz a AKi sorszáma
- A Privi titkos kulcs
- Hitelesítő kód az előző mezőkre

azaz

- Commonname(i)
- i, ENC(AKi, PRIVi)
- MAC BKi.

A kulcsbirtokos azonosítója bármi lehet, ami megfelel az x509v3 tanúsítványformátumnak. Emellett szerepel a cégnél bevezetett univerzális (minden személy-

zeti és jogosultsági adatokat tároló) adatbázisban használt univerzális azonosító is.

A sorszám egy két bájt méretű nem negatív egész.

Az AKi kulcsot az f egyirányú függvénnyel hozzuk létre az AK($i-1$) kulcsból $i > 0$ esetén. Az AKi kulcs mérete 128 bit. Rejtjelző algoritmusként bármelyik modern algoritmus használható, amelyet megfelelő erővel vizsgált a nemzetközi kriptográfus közösség. Elvárásnak tekintjük, hogy blokkos legyen az algoritmus, és a blokkméret legyen legalább 128 bites. Ez a gyakorlatban azt jelenti, hogy valamelyik, az AES projectre készült algoritmust célszerű használni.

Az utolsó mezőben elhelyeztünk egy kontrollösszeget, amely a rekord tartalmát, annak integritását védi szándékos módosítás ellen is. Erre a célra a **HMAC-SHA1** USA-szabvány algoritmust használjuk. A HMAC algoritmushoz az AKi kulcsból származtatott BKi kulcsot használjuk MAC értékként az algoritmus outputjának első 14 bájtját tároljuk le. (Az SHA1 ellen a közelmúltban nyilvánosságra került támadási mód nem veszélyezteti a HMAC részekért történő biztonságos használatot.)

Javasolt megoldásunk főbb pontjai:

- Az installálás folyamán a rendszer generálja a SHARED-MASTERKEY kulcsot, amely 800 bit méretű véletlen sorozat,
- Elkészítjük a templ kulcsot a templ=3DSHA256 [SHARED-MASTERKEY],
- Legyen t=3Dtempl[0]&7,
- A templ értékére végezzük el az SHA256 operációt t-szer egymás után, s az eredmény legyen a 0. rekord rejtjelzésének alapkulcsa. RECORDKEY0 =3DSHA256 t [templ],
- Az i. rekord rejtjelzéséhez az alapkulcsot az előző alapkulcsból kapjuk,
- RECORDKEYi =3D SHA256[RECORDKEYi-1] $i > 0$ esetén,
- Az i. rekord rejtjelzéséhez szükséges kulcsot és kezdővektort a következőképpen kapjuk: (ENCRYPTKEYi IVi) =3D SHA256[RECORDKEYi-1,felhasználó-név]. Itt ENCRYPTKEYi IVi egyaránt 128 bites elemek. A rejtjelzést az AES algoritmussal CBC módban végezzük,
- A sikeres rejtjelzés után $i = 3Di + 1$, kiszámítjuk RECORDKEYi új értékét, és az (i, RECORDKEYi) párost védett formában fájlba is elmentjük.

7. Záró megjegyzések

Dolgozatunkban egy konkrét, hatékony, szimmetrikus kriptográfián alapuló módszert adtunk arra a problémára, hogy a kulcsvisszaállító rendszerekben a rekordok védelmére használt kulcs folyamatosan a memóriában van, ezzel számítástechnikai értelemben veszélyeztetve a biztonságot. A javasolt séma biztosítja, hogy a már letárolt adatok nem fejthetők vissza a gép memóriájában levő éppen aktuális kulcs ismeretében sem.

A séma alkalmazása során egymás után többször hash-elünk viszonylag rövid bitsorozatokat. Az ebből adódható problémák elkerülése miatt választottunk viszonylag hosszú, 256 bites outputtal rendelkező algoritmust.

A témakörhöz tartozó további gyakorlati probléma, hogy mi a teendő akkor, ha az egyik árnyékbirtokos elveszti az árnyékot tartalmazó adathordozót. Erre jelenleg nincs jobb megoldásunk, mint az alaptitok visszaállítása és újraosztása.

Szükséges lenne egy olyan protokoll kidolgozása, amely lehetővé teszi, hogy az árnyék birtokosoknak ne kelljen személyesen, egy időben megjelenni egy felhasználói kulcs visszaállításához.

Hivatkozások

[1] Abelson, H., Ross Anderson, R., Steven M., Bellovin, S. M., Benaloh, B., Blaze, M., Diffie, W., Gilmore, J., Neumann, P. G., Rivest, R. L., Schiller, J. I. and Schneier, B., The Risks of Key Recovery, Key Escrow, and Trusted Third Party Encryption, *The World wide Web Journal* **2/3** (1997).

[2] Dennings, D. and Branstad, D. K., A Taxonomy of Key Escrow Encryption Schemes, *Communications of ACM,* Vol. 39, n. 3.

[3] HMAC, Keyed Hashing and Message Authentication, *FIPS 198* (2002).

[4] Micali, S., Fair Public-Key Cryptosystems, *Laboratory for Computer Science, MIT, Crypto* **92** (Aug. 21, 1992).

[5] 2001. évi XXXV. törvény az elektronikus aláírásról.

[6] Diffie, W. and Hellman, M.E., New directions in cryptography, *IEEE Transactions on Information Theory,* **22** (1976), 644–654.

[7] Rivest, A., Shamir, L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, *Communications of ACM,* Vol. 21, n. 2

[8] Escrowed Encryption Standard (EES), *FIPS 185* (1994).

[9] Shamir, A., How to Share a Secret, *Communications of ACM,* Vol. 22, n. 11

1. Függelék

A CLIPPER project áttekintése

A CLIPPER chip az amerikai NSA által 1993-ban kifejlesztett, alapvetően beszédrejtjelzésre kifejlesztett chip. A chipet az AT&T 3600-as telefonba szánta az NSA. A chip a SKIPJACK nevű algoritmust tartalmazza, amelyet erre a célra fejlesztettek ki. Az algoritmust titokban kívánták tartani, ezért nem esett át nyilvános értékelésen, és a chipet is úgy tervezték hogy a tartalom visszafejtését minél jobban megnehezítsék. Azóta az algoritmust nyilvánosságra hozták. Az algoritmus 64 bites blokkmérettel dolgozó blokkos algoritmus (mint a DES), 80 bit kulcsmérettel, 32 iterációs ciklussal. Sebessége 15 Mbit/sec. A hardware az akkori legmodernebb

(„0.8 mikronos") technológiával a kaliforniai MYKOTRONIX cégnél a legszigorúbb biztonsági, titokvédelmi körülmények között készül. A chip kiolvasás, utólagos megismerés ellen védett. A 80 bites kulcs akkoriban a még regnáló DES algoritmus 56 bites kulcsméretéhez képest meglehetősen sok volt, de a mai gyakorlatban használt legmodernebb algoritmusok minimum 128 bites kulcsához képest meglepően kevés. Az algoritmust Output Feedback módban használták bitfolyam előállítására.

A CLIPPER chip érdekességét a beépített kulcsvisszanyerő módszer adta, amelynek segítségével a tervek szerint az amerikai hatóságok hozzájuthattak volna az aktuális beszélgetés rejtjelzéséhez használt kulcshoz. A koncepció lényeges eleme volt, hogy középtávon csak ilyen chippel ellátott eszközöket lehet majd használni. Az ötlet komoly felzúdulást váltott ki a civil társadalomban, melynek központi kérdése az volt hogy indokolt-e a magánszféra ilyen mértékű korlátozása. Az NSA a koncepció kongresszusi jóváhagyása előtt kiadatta az Escrowed Encryption Standard nevű szabványt (EES.)

Ugyanakkor szakmai vitát is kiváltott a koncepció A kulcsfelfedő rendszer lényege, hogy minden chip rendelkezik egy egyedi azonosítóval, az ennek megfelelő egyedi mesterkulccsal s egy „családi" kulccsal, amely azonos a chipek egy nagy csoportjában. A rejtjelzést kezdeményező chip rendelkezik egy előzetesen kialakított egyszeri kulccsal (session key) amellyel a rejtjelzés történni fog. A rejtjelzés elején a chip létrehoz egy mezőt, (Law Enforcement Field, LEF) amely a következőképpen jön létre; az egyszeri kulcs mesterkulccsal rejtjelzett képe, a chip sorszáma, s néhány bit redundáns információ. Mindezt lerejtjelezzük a családi kulccsal, s megkapjuk a LEF-et. A fogadó chip csak akkor kezdi el a megoldását a kapott rejtjelesnek, ha a megkapott LEF korrekt. Ez azt jelenti, hogy a kapott LEF-et megoldja a családi kulccsal, s az ekkor kapott mezőnek „egy LEF-nek megfelelően kell kinézni." (Pl. ha a LEF-be betett redundáns információ az „USA1993", akkor a fogadó oldal csak akkor fogadja a rejtjelzést, ha a családi kulccsal megoldott LEF-mező végén is ez található.) A hatóságok pedig a chip sorszámának ismeretében adatbázisukból hozzájutnak a chip mesterkulcsához, s ezután a mesterkulcs, s a LEF ismeretében az egyszeri kulcshoz is. Ezután a kommunikáció fejthető. Visszaélések megakadályozására a chip készítésekor a mesterkulcsot két, önmagában semmitmondó komponensre bontják, s két külön adatbázisba helyezik el. A két adatbázist két független, az Igazságügyminiszter által megbízott szervezet birtokolja. Amennyiben bíróság engedélyezi a lehallgatást, a chip sorszámának ismeretében mindkét szervezet átadja a mesterkulcs általa birtokolt komponensét. Arról, hogy a hatóságok az engedély lejárta után ne használják a megkapott mesterkulcsot, rezsim szabályokkal kívántak gondoskodni.

A szakmai és politikai problémák miatt a koncepció nem került át a gyakorlatba, fokozatosan elhalt. A szakirodalomban továbbra is fontos téma egy, minden jelentős követelménynek eleget tevő kulcsvisszaállító rendszer kifejlesztése, de a gyakorlatban a kérdés visszaszorult a vállalati szféra területére.

2. Függelék

Micali fair nyilvános kulcsú rendszere

Micali rendszerének célja egy olyan nyilvános kulcsú infrastruktúra létrehozása, amely az EES-hez hasonlóan lehetővé teszi bizonyos esetekben az államhatalom számára a rejtjelzett üzenetekhez való hozzáférést, ugyanakkor garanciákat is ad arra nézve, hogy ez csak a megfelelő bírósági eljárások után tehető meg. A gondolat lényege, hogy a felhasználók a szokásos PKI rendszerhez hasonlóan generálnak önmaguk számára egy magánkulcs-nyilvános kulcs párt. (Az Elektronikus aláírás törvényben magánkulcsnak nevezik a nyilvános kulcsú rendszerekben használt kulcspárok titokban tartandó részét.) A magánkulcsot több (legyen ez pl. öt) részre osztják, és ezt az öt részt eljuttatják öt különböző megbízotthoz. A szétosztásnak a következő követelményeket kell teljesíteni:

1. Az öt darab birtokában a magánkulcsnak rekonstruálhatónak kell lennie.
2. A magánkulcs ötnél kevesebb darabból nem rekonstruálható. (Ötnél kevesebb darab információelméleti értelemben nem ad információt a magánkulcsról)
3. Minden egyes darabról egyedileg megállapítható, hogy az egy valós, korrekt darabja a magánkulcsnak.

Az utolsó feltétel teljesítése adja a séma erejét. Nyilvánvaló, hogy a magánkulcs ismeretében a darabok korrektsége ellenőrizhető. Azonban ebben a sémában ezt úgy kell megtenni, hogy a megbízottak ellenőrizhessék a hozzájuk eljuttatott darab korrektségét (azaz azt, hogy az öt darabból szükség esetén tényleg előállhat a kulcs), de maguk, sőt ötük közül négyen együtt se juthassak információhoz a magánkulcsról.

Ezek alapján a séma a következő:

- A felhasználók a szokásos módon készítenek maguknak egy kulcspárt. A magánkulcsot öt részre vágják, és egy-egy darabot és a nyilvános kulcsot egy megadott protokoll szerint elküldik az öt megbízottnak.
- Minden megbízott ellenőrzi, hogy a neki eljuttatott darab korrekt-e, és erről értesíti a tanúsítványkibocsátót. (hitelesítésszolgáltatót – HSZ – a magyar terminológiája szerint).
- A HSZ kiadja a felhasználó tanúsítványát a nyilvános kulcsáról, ha mind az öt megbízottól pozitív válasz érkezett.
- Amennyiben bírósági engedély érkezik a felhasználó kommunikációjának lehallgatására, a megbízottak átadják titokdarabjaikat a kormányzatnak, s ezzel lehetővé válik a felhasználó lehallgatása.

A Micali-séma kritikus részének, a titokdarabok megbízottakhoz való eljuttatásának módjának gyakorlati megvalósítása minden rendszerben más. Elvi szinten a főbb lépések a következők:

1. A felhasználó generál egy kulcspárt magának, és annak nyilvános részét átadja a megbízottaknak.
2. Lerejtjelzi, leképezi a magánkulcsot egy adott módon.

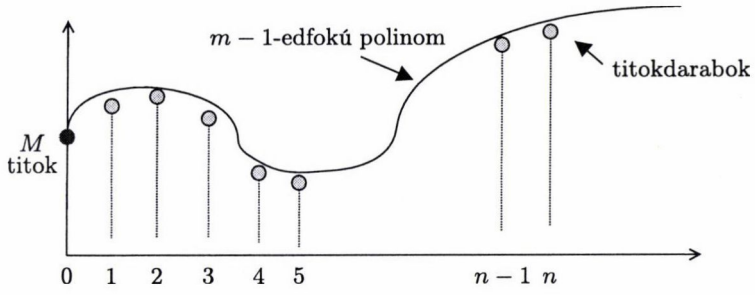
3. A megbízott megkapja a lerejtjelzett képet, és egy Zero-knowledge protokollon alapuló bizonyítékot arról, hogy a rejtjelzés alatt levő kép valóban a megadott nyilvános kulcshoz tartozik.
4. A rejtjelzés alatt levő képet szétosztja egy Verifiable Secret Sharing séma segítségével.

3. Függelék

Shamir-féle titokmegosztási séma

A. Shamir dolgozott ki egy olyan sémát, amellyel egy információ redundánsan többfelé osztható. A feltalált sémát (n, m) küszöbsémának nevezzük $n \geq m$. Lényege, hogy a szétosztandó titokból n darab képet állítunk elő. A darabokat árnyéknak is nevezzük. A szétosztott titok bármely m árnyék birtokában visszaállítható, de $m-1$-ből még nem.

A módszer a Langrange-féle polinominterpoláción alapul. Ennek lényege az, hogy egy $m-1$-edfokú polinom együtthatóit vissza tudjuk állítani, ha ismerjük az m különböző helyen felvett értékét. Legyen a titok a 0 helyen felvett érték, (vagyis a konstans együttható) és legyen a többi együttható véletlenül választott. Ha n részre akarjuk bontani a titkot, akkor legyenek a titokdarabok a polinom $1, 2, \ldots, n$ helyen felvett értékei. Ha az n érték közül tudunk m darabot, s azt, hogy az adott értéket hol vette fel a polinom, akkor a polinom együtthatói visszaállíthatóak. Így a 0. együttható is, ami a titok.



Ha a polinomot véges test fölött tekintjük, akkor az együtthatók értékei korlátosak lesznek, s pontosan látható, hogy mekkora alaptestet kell választanunk ahhoz, hogy egy adott bithosszúságú információt szét tudjunk osztani.

A fentieket konkretizálva, egy lehetséges matematikai keret:

Válasszunk egy p prímszámot, amely nagyobb mint a titok (ha a titkot mint bitekkel felírt számnak tekintjük). Legyen (n) a kiosztandó titokdarabok (árnyékok) száma, és legyen m árnyék szükséges az M titok rekonstruálásához. Véges test feletti algebrai egyenleteket használunk, ami azt jelenti, hogy az alapműveleteket modulo p végezzük el.

A titok megosztásához generáljunk egy tetszőleges $m-1$-ed fokú polinomot a fenti p elemű test felett. Tehát ha egy (n,m)-megosztási sémát akarunk definiálni, akkor generáljunk egy $m-1$-edfokú

$$\left(a_{m-1}x^{m-1}+a_{m-2}x^{m-2}+\ldots+a_1x+M\right) \bmod p$$

polinomot, ahol a p véletlen prím, nagyobb valamennyi generált együtthatónál. Az a_j $(j=1,\ldots,m-1)$ együtthatók véletlenszerűen választottak, titkosak és az árnyékok szétosztása után eldobhatóak. M azonos a titokkal, a p prím akár nyilvánossá is tehető.

Az árnyékokat a polinom n különböző pontban kiszámolt helyettesítési értékeként nyerhetjük:

$$k_i = F(x_i) \bmod p \qquad (i=1,\ldots,n).$$

Más szóval, az első árnyék lehet a polinom értéke az $x=1$ helyen, a második árnyék lehet a polinom értéke az $x=2$ helyen, és így tovább. Ezzel lezártuk a feladat első részét, a titok szétosztását.

Mivel egy $m-1$-edfokú polinomnak m ismeretlen együtthatója van (most: $a_{m-1},\ldots,a_1$ és M), bármely m árnyék segítségével felállítható m lineáris egyenlet, amelyben az együtthatók az ismeretlenek. Ugyanakkor $m-1$, illetve ennél kevesebb árnyék nem elegendő a lineáris egyenletrendszer megoldásához, míg m-nél több árnyék már redundanciához vezet. Ha tehát megoldjuk a lineáris egyenletrendszert (például Gauss-eliminációval), akkor a megoldások között szerepel a nulladfokú tag M együtthatója is. Így megoldottuk a feladat második részét is, visszaállítottuk a titkot. Vegyük észre, hogy nincs szükségünk az összes együtthatóra, csak az M-re. Ez az ötlet gyorsíthatja az egyenletmegoldást.

Egy rövid példán, amelyben n és m értéke nem nagy, szemléletesen bemutatható a fenti séma és megoldása.

Példa egy $(3,5)$-titokmegosztási sémára, amelyben bármely három résztvevő együttesen rekonstruálni tudja az M titkot.

Legyen a titok $M=11$. Legyenek a másodfokú polinom véletlenszerűen választott együtthatói 7 és 8, a véges test elemszáma pedig 13. Tehát a következő másodfokú polinomot generáltuk:

$$F(x_i) = (7x^2+8x+11) \bmod 13$$

A „szétosztott" öt árnyék a következő:

$$k_1 = F(1) = 7+8+11 \equiv 0 \pmod{13}$$

$$k_2 = F(2) = 28+16+11 \equiv 3 \pmod{13}$$

$$k_3 = F(3) = 63+24+11 \equiv 7 \pmod{13}$$

$$k_4 = F(4) = 112+32+11 \equiv 12 \pmod{13}$$

$$k_5 = F(5) = 175 + 40 + 11 \equiv 5 \pmod{13}$$

Rekonstruáljuk az M titkot tetszőleges három árnyékából. Legyenek ezek például k_2, k_3 és k_5. Ekkor a következő lineáris egyenletrendszert kapjuk:

$k_2 = 3$ esetében: $a \cdot 2^2 + b \cdot 2 + M = 3 \pmod{13}$

$k_3 = 7$ esetében: $a \cdot 3^2 + b \cdot 3 + M = 7 \pmod{13}$

$k_5 = 5$ esetében: $a \cdot 5^2 + b \cdot 5 + M = 5 \pmod{13}$

azaz:

$$4 \cdot a + 2 \cdot b + M = 3 \pmod{13}$$

$$9 \cdot a + 3 \cdot b + M = 7 \pmod{13}$$

$$25 \cdot a + 5 \cdot b + M = 5 \pmod{13}$$

A három egyenletből álló egyenletrendszerünk megoldása: $a = 7$, $b = 8$ és $M = 11$. Valóban visszanyertük az M titkot.

A Shamir-féle séma segítségével a résztvevők fontossága, súlya is különböző lehet, ha egyesek egynél több árnyékot kapnak.

A séma nagy hiányossága, hogy feltételezi a résztvevők korrektségét, azaz az árnyékról annak birtokosa nem tudja megállapítani, hogy az valóban a titoknak egy darabja-e, vagy csupán egy véletlen szám. Ezen segítenek az ellenőrizhető titokmegosztási sémák (Verifiable Secret Sharing, VSS)

KEY RECOVERY SYSTEMS IN CRYPTOGRAPHY

PÁL PAPP

One of the most important element of the security of a cryptosystem is the secrecy of the key(s). That is, the key is impossible to recover or to break by an unauthorized entity. However, users may require to recover the key when the key is lost somehow. Similarly, law enforcement agencies may also want to get the key of an ecrypted material. In this paper we will give an overview about the methods avaiable to resolve this „contradicton" flashing the mathematical background too.

In the second part of the paper we focus on a practical problem, and overview the correspondig technical and implementation tasks as well. We have developed a new, symmetric key based method to protect the master key of the key recovery system, which must appear unprotectedly in the RAM of the computer.