

ADATBIZTONSÁG VIZSGA

2009. január 21.

1. Egy bankkártya alkalmazásban 4 decimális karakter hosszú PIN kódot alkalmaznak. Egy támadó kétszer hibázhat, a harmadik sikertelen próbálkozás után a terminál elnyeli a kártyát. Jobb-e ez a rendszer egy kártyatolvaj ellen, mint az, amelyik a 26 betűs angol ábécé betűiből véletlenszerűen sorsolt 3 karakter hosszú jelszót kér hitelesítéskor (kis és nagybetűk egyaránt szerepelhetnek a jelszóban), és a 10. sikertelen próbálkozás után tiltja le a kártyát?
 - a) Adja meg az első rendszerben a tolvaj sikervalószínűségét. (5p)
 - b) Melyik a biztonságosabb rendszer? (Adja meg tolvaj sikervalószínűségét a második rendszerben.) (5p)
2. Adja meg az $x^5=b \pmod{21}$, $0 \leq b \leq 20$ kongruencia egyenlet általános megoldását, azaz egy formulát, ami b ismeretében x értékét megadja. (Segítség: keressen hasonlóságot az RSA-val) (10p)
3. Blokkrejtjelezővel titkosít N blokknyi üzenetet. Az átvitel folyamán egy véletlen blokk beszűrődik az első rejtjelezett blokk első bitje elé. Hány bit lesz véletlenszerűen rossz a dekódolás után, ha a blokk hossza n bit, és a blokkrejtjelező mód
 - a) ECB, (5p)
 - b) CBC, (5p)
 - c) CTR? (5p)A válaszát indokolja képlettel vagy blokkséma részlettel!
4. Tekintsük a digitális aláírást:
 - a) Sorolja fel a digitális aláírás biztonsági tulajdonságait, egy-egy mondattal értelmezve azokat! (5p)
 - b) Hogyan történik az aláírás ellenőrzése hash-and-sign elven működő, publikus kulcsú kriptográfián alapuló séma esetén? (5p)
 - c) Miért készítenek az üzenetről lenyomatot aláírás előtt? Hogyan támadható az aláírás, ha nem ütközésellenálló a hash függvény? (5p)
5. A és B fél az alábbi 4 lépéses protokollt használja kulcsmegegyezésre:
 $A \rightarrow B: A, R_1$
 $B \rightarrow A: B, R_2$
 $A \rightarrow B: A, E_K(R_2)$
 $B \rightarrow A: B, E_K(R_1)$
ahol K egy hosszú távú szimmetrikus kulcs, amelyet csak A és B ismer, E pedig egy biztonságos szimmetrikus rejtjelező. Az alábbi eljárások közül melyeket javasolná a közös ideiglenes ún. session kulcs létrehozására, és melyeket nem? Miért?
 - a) $E_K(R_1+R_2+1)$ (5p)
 - b) $D_K(R_1 \oplus R_2)$ (5p)
 - c) $E_K(K \oplus R_1 \oplus R_2)$ (5p)ahol $+$ operátor az összeadást, míg \oplus operátor a bitenkénti EXOR-t jelenti
6. Kiskérdések
 - a) Mikor beszélünk tökéletes titkosításról? (5p)
 - b) Mire való egy zero-knowledge protokoll? (5p)
 - c) Fermat álprím-e $p-1$ a $b=p-2$ bázisra nézve, ahol p prím, $p>3$? (5p)

Pontozás: 1: <=31, 2: 32 - 43, 3: 44 - 55, 4: 56 - 67, 5: 68 - 80

ADATBIZTONSÁG VIZSGA MEGOLDÁSOK

2009. január 21.

1.
 - a) $1 - (9999/10000) \cdot (9998/9999) \cdot (9997/9998) = 0.0003$ (*).
 - b) A lehetséges jelszavak száma: $a = (26^3) \cdot 2^3 = 140608$. A támadó sikervalószínűsége: $1 - ((a-1)/a) \cdot ((a-2)/(a-1)) \cdot \dots \cdot ((a-10)/(a-9)) = 1 - (a-10)/a = 0.00007112$ (*). Tehát a második rendszer a biztonságosabb. (*)Formailag azonos végeredményt ad (#próbálkozások)/a, de ez nem helyes levezetés!
2. RSA dekódolás feladat. $x=b^d \pmod{21}$, ahol $d=5$. ($5 \cdot 5=1 \pmod{12}$, ahol $12=(3-1)(7-1)$)
3. Blokksémák: Tk 118-139.
 - a) ECB: az első hozzáadott blokk dekódoltja véletlen lesz, a többi blokk helyesen jön ki, csak egy blokk csúszással.
 - b) CBC: az első hozzáadott blokk dekódoltja véletlen lesz, a másodiknak vett blokk is rossz lesz (IV helyett C1-et használ), a harmadik vett bloktól kezdve helyes eredmények jönnek ki egy blokk csúszással.
 - c) CTR: a szinkronizáció elvesztése miatt az üzenet összes blokkja hibás lesz: $N \cdot n$ bit.
4.
 - a)
 - Az aláírás *hiteles*: amikor B ellenőrzi az aláírást A publikus kulcsával, meggyőződik, hogy azt csak A küldhette
 - Az aláírás *nem hamisítható*: csak A ismeri a saját titkos kulcsát
 - Az aláírás *nem újrahazználható* (nem átemelhető másik dokumentumhoz): az aláírás a dokumentum függvénye is
 - Az aláírt dokumentum *nem módosítható*: ha módosítják a dokumentumot, az eredeti aláírás nem illeszkedik, s ez detektálható
 - Az aláírás *letagadhatatlan*: B vagy egy harmadik fél A közreműködése nélkül ellenőrizni képes az aláírást
 - b) Az aláírást ellenőrző fél az aláíró nyilvános kulcsával dekódolja az aláírást és elkészíti az üzenet lenyomatát (ugyanazt a hash eljárást alkalmazva, mint az aláíró) és a két eredményt összeveti. Egyezés esetén az aláírást hitelesnek fogadja el.
 - c) nem nehéz feladat olyan X, X' ($X; X'$) üzenetpárt megadni, amelyeknek azonos a lenyomata, azaz amelyekre $H(X)=H(X')$; $D_A(H(X))=D_A(H(X'))$
támadás: $[X, D_A(H(X))], [X', D_A(H(X))]$
5.
 - a) nem javasolt, mivel a támadó ismeri R_1, R_2 -t, és így az R_1+R_2+1 az 1. vagy a 2. lépésben el tudja küldeni valamelyik félnek, ami visszaküldi $E_k(R_1+R_2+1)$ -t
 - b) javasolt, mivel egyik fél sem hajt végre dekódolást, a K kulcsot pedig a támadó nem ismeri
 - c) javasolt, mivel a támadó nem ismeri a K kulcsot, így az a) esetenél látott támadás nem kivitelezhető
6.
 - a) Tökéletes titkosítás (Tk.19.o): Akkor beszélünk tökéletes titkosításról, ha az X és Y valószínűségi változók statisztikailag függetlenek, azaz kölcsönös információjuk zérus, $I(X,Y)=0$
 - b) Zero-knowledge protokoll segítségével A úgy tudja valamilyen információ birtoklását bizonyítani B felé, hogy B nem tud meg semmit az információról konkrétan, csak a birtoklás tényét.
 - c) Nem. $(p-2)^{p-2} = (-1)^{p-2} = -1 \pmod{p-1}$, ($p-2$ páratlan).