HIBAJEGYZÉK

A következő bekezdésekben a 2004. februárjában megjelent „Titkosítás és adatrejtés” című könyvben felfedezett hibákat gyűjtöttem össze.

A 9. oldal 16. sorában:

Az lehetséges kulcsok halmazát kulcstérnek nevezzük.

helyesen:

A lehetséges kulcsok halmazát kulcstérnek nevezzük.

A 15. oldal 3. és 4. sorában:

Assume your adversaries are better than thay are. Assume science and technology will soon be able to do thins they cannot yet.

helyesen:

Assume your adversaries are better than they are. Assume science and technology will soon be able to do things they cannot yet.

A 39. oldalon kezdődő és a 40. oldalon befejeződő mondat:

A rendszernek mindegy egyes átvitt üzenetszimbólumhoz...

helyesen:

A rendszernek minden egyes átvitt üzenetszimbólumhoz...

Az 51. oldal 31. sorában:

... de ha van korlát csak korhadt, azonban ez nem látszik rajra ...

helyesen:

... de ha van korlát csak korhadt, azonban ez nem látszik rajta ...

A 68. oldal 21. lábjegyzethivatkozása:

http://www.setiathome.ssl.berkely.edu

helyesen:

http://www.setiathome.ssl.berkeley.edu

A 69. oldal 23. sorában:

Az fenti időpontok, időtartamok...

helyesen:

A fenti időpontok, időtartamok...

A 69. oldal 34. sorában:

Az EEF már 1997-ben elkezdett...

helyesen:

Az EFF már 1997-ben elkezdett...

A 88. oldal 26. sorában:

...az egyel korábbi...

helyesen:

...az eggyel korábbi...

A 101. oldal 12. sorában:

...és a közös titkok nem feltétel...

helyesen:

...és a közös titok nem feltétel...

A 113. oldal 8. sorában:

Binary extended Eudidean GCD algorithm

helyesen:

Binary extended Euclidean GCD algorithm

A 146. oldal 5. sorában:

Néhány gyakorlati indok az áttérés mellet:

helyesen:

Néhány gyakorlati indok az áttérés mellett:

A 149. oldal 20. sorában:

... problémáját oldatta meg.

helyesen:

... problémáját oldotta meg.

A 180. oldal 20. sorában:

... kimeneti 64 bitből csak eggyet használunk fel.

helyesen:

... kimeneti 64 bitből csak egyet használunk fel.

A 200. oldal 10. sorában:

Másrész hiányzik...

helyesen:

Másrészt hiányzik...

A 200. oldal 25. sorában:

...certficate ...

helyesen:

...certificate ...

A 213. oldal 31. sorában:

...collision resistane...

helyesen:

...collision resistance...

A 217. oldal 6. sorában:

... teszzük, mint ahogy...

helyesen:

... tesszük, mint ahogy...

227. oldal, 52. ábra

Alice és Bob arcán látható nyíl értelem nélküli, felesleges.

228. oldal, 53. ábra

Alice arcán látható nyíl értelem nélküli, felesleges.

A 231. oldal 25. sorában:

... (know plaintext attack)...

helyesen:

... (known plaintext attack)...

233. oldal

A születésnapi paradoxon példáinak számítása helyesen a következő:

A1. Hány embernek kell együtt lennie ahhoz, hogy egy kiválasztott ember születésnapja legalább 50%-os valószínűséggel megegyezzen egy adott dátummal?

Fordítsuk meg előbb kérdést: milyen valószínűséggel áll elő az a helyzet, hogy senkinek sem egyezik meg a születésnapja? Az első embernek erre $\frac{364}{365}$ esélye van. A másodiknak, a harmadiknak, a negyediknek szintén. Annak valószínűségét, hogy az elsőnek sem, **és** a másodiknak sem, **és** a harmadiknak sem „nyerő” a születésnapja, ezen esélyek szorzataként számíthatjuk ki: $\left(\frac{364}{365}\right)\left(\frac{364}{365}\right)\left(\frac{364}{365}\right)\ldots$ vagyis n fő esetén $\left(\frac{364}{365}\right)^n$. Annak valószínűsége,

hogy a fenti, sajnálatos esemény (miszerint senkinek sem passzol a születésnapja) mégsem következik be: $1-\left(\frac{364}{365}\right)^n$ és ez *n=253*-nál lesz először nagyobb, mint 50%. (Érdekességképpen: *n=840* fő esetén, több mint *90%* a siker esélye, *n=1092* fő esetén *95%*, és *n=1679* fő esetén *99%*.)

A2. Hány embernek kell együtt lennie ahhoz, hogy közülük tetszőleges kettőnek legalább 50%-os valószínűséggel megegyezzen a születésnapja?

Az iménti gondolatmenethez hasonlóan fordítsuk meg ismét az eredeti kérdést, vagyis milyen valószínűséggel fordul elő, hogy nincs két azonos születésnapú ember a csoportban?

Az első ember születésnapja az év bármely napjára eshet, ő egymagában még nem ütközik senkivel. A másodiknak már csak 364 napja marad (mert egy már foglalt), így az ő esélye arra, hogy a születésnapja nem ütközik az első emberével: $\frac{364}{365}$. A harmadik embernek már csak 363 olyan nap maradt, ami nem ütközik az eddigi résztvevőkével, így az ő esélye egy nem ütköző születésnapra: $\frac{363}{365}$. Annak valószínűsége, hogy minden résztvevő születésnapja más és más napra esik, az iménti esélyek szorzataként számítható ki: $\frac{365}{365}*\frac{364}{365}*\frac{363}{365}*\ldots$ vagyis *n* fő esetén $\frac{365}{365}*\frac{364}{365}*\frac{363}{365}*\ldots*\frac{366-n}{365}=\frac{365!}{(365-n)!*365^n}$. Ez egy meglehetősen ronda tört, tele van faktoriálissal és az ismeretlen *n* is rendesen elbújt benne... Akik lépten-nyomon ilyen feladatot oldanak meg, az alábbi egyszerűbb és sokkal könnyebben számolható közelítést szokták alkalmazni:

$\frac{365!}{(365-n)!*365^n}\approx e^{-n^2/(2*365)}$ Annak valószínűsége, hogy a fenti, sajnálatos esemény (miszerint egyetlen párost sem találunk) mégsem következik be: $1-e^{-n^2/(2*365)}$. Ez a valószínűség először *n=23* fő esetén lesz nagyobb, mint 50%. (Érdekességképpen: *n=41* fő esetén, több mint *90%* a siker esélye, *n=46* fő esetén *95%*, és *n=58* fő esetén már *99%*.)

A fenti kérdések az üzenetpecsétekre vonatkozóan a következőképpen néznek ki (egy 128 bites üzenetpecsétjét feltételezve):

B1. Ha adott egy X_1 üzenet, hány X_2 üzenetet kell generálni, hogy az X_2 üzenetek között k valószínűséggel legyen legalább egy olyan, aminek pecsétje megegyezik X_1 pecsétjével? (Vagyis egy olyan üzenetet keresünk, melynek pecsétje adott.)

$$1-\left(\frac{2^{128}-1}{2^{128}}\right)^n \geq k$$

Ennek a keresésnek *k=99.9%* esetben is olyan nagy időigénye van, hogy a gyakorlatban nem kivitelezhető (több milliószor milliárd év).

B2. Néhány esetben egy protokoll támadásához az is elég, ha találunk két olyan X_1 és X_2 közömbös tartalmú üzenetet, melyek kötetlenek, csak pecsétjük legyen azonos. Hány üzenetpárt kell generálni, hogy k valószínűséggel legyen közöttük jó páros?

$$1-e^{-n^2/(2*2^{128})} \geq k \qquad \Rightarrow \qquad n \geq \sqrt{2*\ln\frac{1}{1-k}}\sqrt{2^{128}}$$

Legyen *k=99.9%*, ekkor $n=3{,}7169 * 2^{64}$ üzenetet kell generálni. Ez már nem is olyan sok, mondjuk 1 millió pecsétpáros/másodperc sebességet feltételezve mindössze 2,1 millió év.

Ha a vizsgált üzenetpecsét hossza nem 128 bites, hanem csak 64 bites lenne, a két időtartam B1=9,3 millió év és B2=4,4 óra (!!!) lenne. Ez a különbség már jóval érzékelhetőbb, és sokkal veszélyesebb is. A kapott eredmény „formája” miatt „négyzetgyök-támadásnak” (*square root attack*) is nevezik.

A 239. oldal utolsó előtti sorában:

... nem veszzük figyelembe...

helyesen:

... nem vesszük figyelembe...

A 271. oldal 20. sorában:

... Direcytory Security fülre.

helyesen:

... Directory Security fülre.

A 272. oldal 7. sorában:

... aki majd ellenőrzi adatok...

helyesen:

... aki majd ellenőrzi az adatok...

A 273. oldal 13. sorában:

... üzemeltetjük, hanem subordiante CA-ként...

helyesen:

... üzemeltetjük, hanem subordinate CA-ként...

A 319. oldal utolsó sorában:

Confidentality...

helyesen:

Confidentiality...

A 330. oldal 6. sorában:

Három darab DES egymás utáni használta egy adatblokkon.

helyesen:

Három darab DES egymás utáni használata egy adatblokkon.

A 75. oldal 18. sora, illetve a 75. oldal alulról a második sor

Bruce Schneier neve helyesen: Bruce Schneier. (Köszönet Bitman-nek)

A 230. oldal alulról a 11. sor

„reply attack” helyesen „replay attack” (Köszönet Bitman-nek)

252. oldal

Az fLen definíciója helyesen: „Formátumleíró rész (a következő 16 bájt) hossza.” (Mert ez a 8 darab 2 bájtos mező az „FMT_” chunk tartalma.) (Köszönet Bitman-nek)