Errata

Errata za "Kriptografija", Element, 2007.

Zahvala

Ivan Stanković,
Zoran Dodlek,
Bernardin Ibrahimpašić,
Borka Jadrijević

Poglavlje 1.

⋆ Str. 21, 3. red

Treba pisati:
"Npr. za $j = 1$ i $g = 0$ je . . . "

⋆ Str. 53, zadatak 8.c)

Šifrat u c) zadatku je šifriran supstitucijskom šifrom, a ne Vigenereovom kako piše u zadatku.

⋆ Str. 62

"Bitove ključa najprije permutiramo permutacijom PC2 - redoslijed bitova je (14, 17, 11, ...)."
Umjesto PC2 treba pisati PC1.

⋆ Str. 75, tablica

Nedostaje redak za 0001.

0001	000011, 001111, 011110, 011111, 101010, 101011, 110111, 111011

Poglavlje 2.

★ Str. 92, primjer 2.8 (AES)

Matrica k u sredini stranice ima greške u zadnjem stupcu u dva predzadnja retka. Treba pisati:

$$k = \begin{pmatrix} ab & 23 & 98 & 10 \\ cd & 45 & 76 & fe \\ ef & 67 & 54 & \mathbf{dc} \\ 01 & 89 & 32 & \mathbf{ba} \end{pmatrix}$$

★ Str. 93, runde AES-a

Zadnja matrica pri dnu stranice ima greške u zadnjem stupcu u dva predzadnja retka. Treba pisati:

$$s \oplus k = \cdots = \begin{pmatrix} ab & 23 & 98 & 10 \\ cd & 45 & 76 & fe \\ ef & 67 & 54 & \mathbf{ec} \\ 01 & 89 & 32 & \mathbf{8d} \end{pmatrix}$$

Poglavlje 3.

★ Str. 119, prvi odlomak u 3.3.3

"Najefikasniji poznati algoritmi za problem diskretnog algoritma u grupi . . . "

(diskretnog algoritma → diskretnog logaritma)

★ Str. 122, prvi odlomak

rečenica "Među konačnim poljima, pored polja Z_p, najvažija su polja karakteristike 2."

(najvažija→ najvažnija)

★ Str. 124, 4. odlomak

rečenica "Danas se najboljim smatra Pollardova . . . "

(najboljim → najboljom)

★ Str. 125, 4. odlomak

rečenica "Međutim, postoje tipovi eliptičkih krivulja kod kojih je taj problem nešto (ali čak puno) lakši."
(ali čak → ili čak)

★ Str. 125, 2. točka na dnu stranice

rečenica "Stoga se analomalne krivulje. . . "

(analomalne → anomalne)

★ Str. 135, treći odlomak

rečenica "Tada Alice pošalje Bobu šifrat

$$y = (0, 0, 0, 1, 1, 0, 0,).$$

(zarez iza zadnje nule je suvišan)

Poglavlje 4.

★ Str. 149, definicija 4.1

"(Shannova entropija)"

(Shannova → Shannonova)

★ Str. 152, 2. odlomak

"Ako je $(x/n) = -1$, onda smo sigurni da n nije kvadratni ostatak."

(sigurni da n nije → sigurni da x nije)

Poglavlje 5.

★ Str. 154, prvi odlomak

"Važan teoretski rezultat o BBS generatoru... prethodnika za BSS generator..."

$(BSS \to BBS)$

★ Str. 158, algoritam 13

U 4. koraku algoritma umjesto "mod n" treba pisati "mod q".

★ Str. 171, algoritam 16

redak 4., umjesto

$$\mathsf{else}\ w_i = x_i + y_i + c; c = 1$$

treba glasiti

$$\mathsf{else}\ w_i = x_i + y_i + c - b; c = 1$$

★ Str. 172, odlomak iza algoritma 18

"Najbolji poznati algoritmi za množenje i zbrajanje imaju složenost ..."

(zbrajanje → dijeljenje)

★ Str. 175, algoritam 19

U 7. liniji algoritma

$$p \to m$$

★ Str. 180, definicija Fibonaccijevih brojeva u središnjem odlomku

Umjesto:

$$F_n = F_{n-1} + F_{n+2}$$

treba biti:

$$F_n = F_{n-1} + F_{n-2}$$

★ Str. 181, 3. red

U formuli za $P(q)$, umjesto $\log_2(1-\dots)$, treba pisati $\log_2(1+\dots)$

⋆ Str. 209, prvi odlomak

"Dakle, postavlja se pitanje postoji li točka $P \ldots$ čiji je red P veći od $\ldots$ "

(red P veći $\rightarrow$ red veći)

⋆ Str. 209, drugi odlomak

"To znači da ako znamo red od $\#E(F_p)$, onda znamo i red od $\#E'(F_p)$, i obrnuto."

(suvišno je '#')

⋆ Str. 224, lema 5.22

"*Dokaz.* Za $0 < i < n$ je koeficijent od X^i u polinomu $((X + a)^n - (X^n - a))$ jednak $\ldots$ "

Trebalo bi pisati:

$$((X + a)^n - (X^n + a))$$