Bernasconi, Ferragina, Luccio. Elementi di Crittografia
Errata corrige

p. 20 riga 11 dal fondo

si ottiene immediatamente AGGIUNGERE per $N \geq 2$

p. 44 riga 20

3,2,1 - 3,1,2 DIVIENE 3,1,2 - 3,2,1

p. 66 riga 3 dal fondo (nella nota)

molto maggiore del valore $3N/4$ derivante dal lemma

DIVIENE molto minore del valore $N/4$ stabilito nel lemma

p.73 riga 16 dal fondo

"ZI OREGAR GNBUR" DIVIENE "ZI ORDGAR GNLUR"

p.76 riga 10 dal fondo (esclusa nota)

"indice mobile DIVIENE "indice mobile"

p. 88 riga 11 dal fondo

"rompere DIVIENE "rompere" (mancano virgolette)

p. 99 due righe finali (nella nota)

lunghezza n perché tra questi si trovano anche tutti

DIVIENE lunghezza n anche perché tra questi si trovano tutti

p. 134 righe 8-12

Anche la scelta di e deve avvenire oculatamente. Anzitutto […] trasformazione del messaggio.

DIVIENE

Anche la scelta di e deve avvenire oculatamente. Anzitutto se k è un divisore sia di $p-1$ che di $q-1$ (si noti che $p-1$ e $q-1$ sono entrambi divisibili per 2), e se m,n sono primi tra loro, si può dimostrare che per $e = 1+\Phi(n)/k$ si avrebbe $c = m^e \bmod n = m$; quindi tale valore non indurrebbe alcuna trasformazione del messaggio.

p. 195 fase **broadcast** di **bitcoin**

La coppia <m,h> DIVIENE La coppia <m,f>

p. 209 riga 6 dal fondo

un quarto della chiave DIVIENE metà della chiave

si noti infatti che la chiave è costituita da metà della sequenza originale

p. 210 riga 9 colonna 2 Figura 11.4

↗ DIVIENE ↘

p. 216 riga 15

(paragrafo ??) DIVIENE (paragrafo 8.4)