

Crittografia: ERRATA CORRIGE

Ferragina, Luccio

p 52 r -15. $P_{\text{zaino.max}}(I,b,c) \Rightarrow P_{\text{zaino.max}}(I,c)$

p 58 r -8. $T/S \leq \Rightarrow T/S <$

p 63 r -7. $q \bmod 4 = 3$, e sia

$\Rightarrow q \bmod 4 = 3$, $2^{\lfloor p/4 \rfloor + 1}$ e $2^{\lfloor q/4 \rfloor + 1}$ siano primi e sia

p 66 r 17. $1 \leq y \leq N-1 \Rightarrow 2 \leq y \leq N-1$

p 66 r -6, p 67 r -3. a caso tra 1 e $N-1 \Rightarrow$ a caso tra 2 e $N-1$

p 69 r 1/2. il bit più significativo è uguale a 1

\Rightarrow i due bit estremi sono uguali a 1

p 69 r 4. $N \leftarrow 1S$, ove S è una sequenza di $n-1$ bit

$\Rightarrow N \leftarrow 1S1$, ove S è una sequenza di $n-2$ bit

p 69 r 6. do $N \leftarrow N+1 \rightarrow$ do $N \leftarrow N+2$

p 99 r 7. delle chiavi.

\Rightarrow delle chiavi, caratteristica per nulla ovvia vista la struttura del cifrario.

p 102 r 17. AGGIUNGERE:

I blocchi EP e S sono studiati in modo che tutti i bit di $D[i-1]$ influenzino l'uscita di S , senza di che non sarebbe poi possibile

decifrare

il messaggio.

p 109 didasc. fig. 7.8. indicare il bit \Rightarrow indicare il blocco

p 114 r -15. La proprietà 2 \Rightarrow La proprietà 2a

p 116 r 8. per ogni $a \notin \mathbb{Z}_n^*$ (quindi a primo con n)

\Rightarrow per ogni a primo con n

p 117 r 7. $d',x',y' \Rightarrow d',y',x'$

p 117 r 9. restituisce la tripla \Rightarrow restituisce una delle triple