pg.	onde se lê	leia-se
38	Se $r_0 = r_n$, ... é zero	Se $r_0 = r_n$, ... é um
38	Se $r_0 << r_n$, ...	Se $r_0 >> r_n$, ...
39	... correta com significado.	...correta com significado. Se $2^{E(K)-n_0 d} = 2^0 = 1$, então só um legível é obtido, e é o correto.
50	3. Cada ... entre 0 e 255, *i.e.*, ...	3. Cada ... entre 0 e 15, *i.e.*, ...
102	...$p = s^{-1} \bmod n$ (por exemplo...	...$p = s^{-1} \bmod \Phi(n)$ (por exemplo...
103	... pois chave (s, n) pode ser ...	... pois chave (p, n) pode ser ...
108	Como $m = tr$ ...	Como $m = tq$ ...
109	3. Finalmente ... da diferença de ...	3. Finalmente ... da soma de ...
114	Seja $n = 2^t c$, onde ...	Seja $n - 1 = 2^t c$, onde ...
129	$\{\beta, \beta^2, \beta^{2^2}, ...\beta^{2^{m-1}}\}$	$\{\beta, \beta^2, \beta^{2^2}, ...\beta^{2^{m-1}}\}$
129	$\alpha^2 = \sum_{j=0}^{m-1} b_j \beta^{2^j+1} = \sum_{j=0}^{m-1} b_{j-1} \beta^{2^j}$	$\alpha^2 = \sum_{j=0}^{m-1} b_j \beta^{2^{j+1}} = \sum_{j=1}^{m} b_{j-1} \beta^{2^j}$
140	$y^2 + cy = (x^3 + ax^2 + b) \bmod 2^m$	$y^2 + cy = (x^3 + ax + b) \bmod 2^m$
141	... um inteiro k e calcula ...	... um inteiro $k : 1 < k < 2^m$ e calcula ...
144	... o contrapositivo. Se $x_j = 0$ e ...	... o contrapositivo. Se $u_j = 0$ e ...
143	A chave secreta $S_{Alice} = (m, r, A')$ é ...	A chave secreta $S_{Alice} = (m, w, A')$ é ...
145	1.1 **se** $y' > a'_j$	1.1 **se** $y' \geq a'_j$
145	1.2 **senão** $u_j \leftarrow 0$;	1.2 **senão** $u_j \leftarrow 0$; }
145	1.5 }	
146	2. A chave ... ($m = 127$, ...	2. A chave ... ($m = 627$, ...

pg.	onde se lê	leia-se
157	$= r^v[(s_A)^s(s_A)^v]^e \bmod n$	$= r^v[J_A(J_A^{-s})^v]^e \bmod n$ $= r^v[J_A J_A^{-sv}]^e \bmod n$ $= r^v[J_A J_A^{-1}]^e \bmod n$
170	... satisfizer $1 \leq z \leq (p-1)$ ...	... satisfizer $1 \leq y \leq (p-1)$ ...
172	2. A seguir calcula $y' = yu \bmod (p-1)$ e z' tal ...	2. A seguir calcula $z' = zu \bmod (p-1)$ e y' tal ...
172	...$z' = zu \bmod (p-1)$ e $z' = z \bmod p$ (este z' pode ...	...$y' = yu \bmod (p-1)$ e $y' = y \bmod p$ (este $y' \bmod p(p-1)$ pode ...
172	3. O par ...$1 \leq z' \leq p-1$.	3. O par ...$1 \leq y' \leq p-1$.
175	$((g^x g^{SC})^{D^{-1} mod\ q} \bmod p) \bmod q \quad =$	$((g^x g^{SC})^{D^{-1} mod\ q} \bmod p) \bmod q \quad =$ pois $T = g^S \bmod p$
205	... Z_p^* possui um gerador.	... Z_p^* possui $\Phi(p-1)$ geradores.
208	x ... 6 ... $x^2 = a \bmod 15$ ... 9 ...	x ... 6 ... $x^2 = a \bmod 15$ ... 6 ...
208	... quadradas de 5 módulo 41 são 5 e 13	... quadradas de 5 módulo 41 são 28 e 13
209	A seguir, pelo Teorema Chinês ...	$(a^{(p-1)/2} = -1 \bmod p \Rightarrow a$ não é resíduo quadrático $\Rightarrow a$ não possui raiz quadrada) A seguir, pelo Teorema Chinês ...
210	1. $p\|x-y\|$	1. $p\|x-y$
211	2.3 /* tem-se aqui ...	2.3 } /* tem-se aqui ...

O exemplo na página 146 corrigido para o valor $m = 627$ é como segue:

1. Vamos supor que o texto legível a ser enviado por Beto seja $x = (01011001)$.

2. A chave secreta da Alice para $n = 8$ é
   $(m = 627,\ w = 431,\ A' = (3, 5, 9, 18, 37, 75, 148, 298))$.

3. A chave pública da Alice é: $A = (a_1 = 431 * 3 \bmod 627 = 39, a_2 = 431 * 5 \bmod 627 = 274, a_3 = 431 * 9 \bmod 627 = 117, a_4 = 431 * 18 \bmod 627 = 234, a_5 = 431 * 37 \bmod 627 = 272, a_6 = 431 * 75 \bmod 627 = 348, a_7 = 431 * 148 \bmod 627 = 461, a_8 = 431 * 298 \bmod 627 = 530)$,
   i.e., $A = [39, 274, 117, 234, 272, 348, 461, 530]$

4. Beto calcula o texto ilegível $y = 0 * 39 + 1 * 274 + 0 * 117 + 1 * 234 + 1 * 272 + 0 * 348 + 0 * 461 + 1 * 530 = 1310$ e envia y para Alice

5. Alice recebe y e conhecendo a chave secreta ($m = 627$, $w = 431$, $A' = (3, 5, 9, 18, 37, 75, 148, 298)$) efetua os seguintes cálculos::

    1. Calcula $w^{-1} \bmod m = 431^{-1} \bmod 627 = 611$;
    2. Calcula $y' = 1310 * w^{-1} \bmod m = 1310 * 611 \bmod 627 = 358$;
    3. Resolve a equação $358 = u_1 * 3 + u_2 * 5 + u_3 * 9 + u_4 * 18 + u_5 * 37 + u_6 * 75 + u_7 * 148 + u_8 * 298$
    4. A solução é: (01011001)