正誤情報

このたびは森北出版株式会社発行の書籍をお買い求めいただき、誠にありがとうございました. 下記の書籍につきまして誤りのある箇所がございましたので、お詫びし訂正させていただきます.

2015年2月16日 森北出版株式会社 生産マネジメント部

タイトル

Javaで作って学ぶ暗号技術

正誤対象

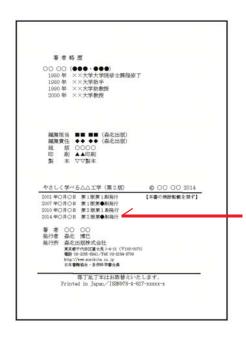
お手持ちの書籍の刷数をお調べのうえ,下の表をご覧下さい.正誤表内の一番左に「対応刷数」という列がございます.該当する刷数の訂正情報をご参照下さい.

なお, 刷数につきましては下記「刷数の調べ方」をご参照ください.

お持ちの本の刷数				
1	対応刷数 1 より 2 をご参照ください			
2	対応刷数 2 をご参照ください			
それ以降	現在把握している訂正情報はございません			

刷数の調べ方

本の一番後ろのページ(広告等除く)に下図のようなページがございます. ご参照いただき, お持ちの本の刷数をお調べください.



日付の最も新しい行に記載された数字がお持 ちの本の刷数となります

対応刷数	頁	行数, 図・表・ 式番号	誤	正
2	7	15 行目	…30 個の 2.2GHz opteron プロセッサを持つ…	…30 個の 2.2GHz AMD Opteron(TM)プロセッサを持つ…
2	18	下から 6 行目	…意味で「本物の」乱数です. IC カードなどには真性乱数生成装置が内蔵されていることがあります.	…意味で「本物の」乱数です.真性乱数生成装置は,単体で製品としても 販売されています.
2	36	21 行目	…計算終了を待たずにプログラムの実行を中止させています.後 で説明しますが,…	…計算終了を待たずに CTRL+C キーを押して, プログラムの実行を中止させています(そのため, "^C"という文字が現れています). 後で説明しますが, …
1	41	1~5 行目	<pre>for (BigInteger r = a.remainder(b); !r.equals(BigInteger.ZERO);){ // [STEP 1-1], [STEP 1-2] a = b; b = r; }</pre>	<pre>for (BigInteger r = a.remainder(b); !r.equals(BigInteger.ZERO);</pre>
1,2	117	⊠ 4.3	RKN, ラウンド AddRoundKey	INPUT 第1ラウンド AddRoundKey InvShiftRows InvSubBytes RK ₁ AddRoundKey RK ₂ InvMixColumns InvShiftRows InvSubBytes RK _N InvSubBytes

1	124	下から 5 行目	…ステートの並び順を列方向にシフトする処理…	…ステートの各行を列方向にずらす処理…
1	124	脚注 *6	"row"は列という意味です.	"row"は行という意味です.
1	128	4 行目	o0~o4 という変数は…	o0~o3 という変数は…
1	128	5 行目	t0~t4 という変数は…	t0~t3 という変数は…
1	128	9 行目	・・・・位置には 0_n ^ 0_n がセットで・・・	・・・・位置には \mathbf{o}_n t $_n$ がセットで・・・
1	132	4 行目	$RK_2 = \cdots$	$RK_1 = \cdots$
1	132	6 行目	$\cdots W_{N_r+2} W_{N_r+3}$	$\cdots W_{4N_r+2} W_{4N_r+3}$
1	133	下から 8 行目	\cdots , P_1 , P_2 , \cdots	\cdots , P_0 , P_1 , \cdots
1	139	下から 2 行目	\cdots , T_1 , T_2 , \cdots	\cdots , T_0 , T_1 , \cdots
1	140	1, 2, 4, 5 行目	$j=1,2,\cdots$	$j=0,1,\cdots$
2	159	6 行目	…設定しています. k_0 の 0 によるパディングは, 最初に k_0 を 0 で初期化し	…設定しています. K_0 の 0 によるパディングは、最初に K_0 を 0 で初期化し
1	166	最下行	同時, クライアントに…	同時にクライアントに…
1	175	下から 11 行目	続く 0100 が…	続く 01 以降が…
2	198	16 行目	…の引数や, pad_1, pad_2 の長さに…	…の引数や, pad1, pad2 の長さに…
2	205	下から 14 行目	最後にサーバ 1Finished メッセージを送信します	最後にサーバは Finished メッセージを送信します