

This is the errata for the book

Cryptography and Embedded Systems Security, Xiaolu Hou, Jakub Breier, ISBN: 978-3-031-62205-2, Springer Nature, 2024.
published version

<https://link.springer.com/book/10.1007/978-3-031-62205-2>

The author’s copy with errors corrected can be found in the following link:

<https://xiaoluhou.github.io/Textbook.pdf>

Location	Original	Change																														
Page 9, Algorithm 1.1, lines 2-4	<div><div><div><div><div><div></div><div>Input: $m, n // m, n \in \mathbb{Z}, m \neq 0$</div><div>Output: $\gcd(m, n)$</div></div></div><div><div>1</div><div>while $m \neq 0$ do</div></div><div><div>2</div><div>$r = n \% m //$ remainder of n divided by m</div></div><div><div>3</div><div>$n = m$</div></div><div><div>4</div><div>$m = r$</div></div></div><div><div>5</div><div>return r</div></div></div></div>	<div><div><div><div><div><div></div><div>Input: $m, n // m, n \in \mathbb{Z}, m \neq 0$</div><div>Output: $\gcd(m, n)$</div></div></div><div><div>1</div><div>while $m \neq 0$ do</div></div><div><div>2</div><div>$r = m$</div></div><div><div>3</div><div>$m = n \% m //$ remainder of n divided by m</div></div><div><div>4</div><div>$n = r$</div></div></div><div><div>5</div><div>return n</div></div></div></div>																														
Page 18, first paragraph below Definition 1.2.12	By definition, for any $a \in F$, there exists $b \in F$ such that ...	By definition, for any $a \in F$, $a \neq 0$, there exists $b \in F$ such that ...																														
Page 20, Example 1.2.24	$f(1 \oplus 0) = f(1) = a, f(1) + f(0) = a + b = a$	$f(1 \oplus 0) = f(1) = b, f(1) + f(0) = b + a = b$																														
Page 49, Theorem 1.5.1	of $\deg(f(x)) \geq 1$	if $\deg(f(x)) \geq 1$																														
Page 51, Example 1.5.6	<div>$\mathbb{F}_2[x]/(f(x)) = \{1, x, x + 1\}$... $\mathbb{F}_2[x]/(g(x)) = \{1, x, x + 1\}$</div>	<div>$\mathbb{F}_2[x]/(f(x)) = \{0, 1, x, x + 1\}$... $\mathbb{F}_2[x]/(g(x)) = \{0, 1, x, x + 1\}$</div>																														
Page 106 Table 2.2 (b)	<table><tr><td>\acute{A}</td><td>11000001</td><td>C1</td></tr><tr><td>\ddot{A}</td><td>11000100</td><td>C4</td></tr><tr><td>\acute{I}</td><td>11001101</td><td>CD</td></tr><tr><td>\times</td><td>11010111</td><td>D7</td></tr><tr><td>\div</td><td>11110111</td><td>F7</td></tr></table>	\acute{A}	11000001	C1	\ddot{A}	11000100	C4	\acute{I}	11001101	CD	\times	11010111	D7	\div	11110111	F7	<table><tr><td>\acute{A}</td><td>1100001110000001</td><td>C381</td></tr><tr><td>\ddot{A}</td><td>1100001110000100</td><td>C384</td></tr><tr><td>\acute{I}</td><td>1100001110001101</td><td>C38D</td></tr><tr><td>\times</td><td>1100001110010111</td><td>C397</td></tr><tr><td>\div</td><td>1100001110110111</td><td>C3B7</td></tr></table>	\acute{A}	1100001110000001	C381	\ddot{A}	1100001110000100	C384	\acute{I}	1100001110001101	C38D	\times	1100001110010111	C397	\div	1100001110110111	C3B7
\acute{A}	11000001	C1																														
\ddot{A}	11000100	C4																														
\acute{I}	11001101	CD																														
\times	11010111	D7																														
\div	11110111	F7																														
\acute{A}	1100001110000001	C381																														
\ddot{A}	1100001110000100	C384																														
\acute{I}	1100001110001101	C38D																														
\times	1100001110010111	C397																														
\div	1100001110110111	C3B7																														
Page 133	When $\omega_1 = \omega_2...$ the Sbox is a ω_1 –bit Sbox	When $\omega_1 = \omega_2...$ the Sbox is an ω_1 –bit Sbox																														
Page 139, RSA security	Nevertheless, post-quantum public key cryptosystems are being proposed (see e.g. [HPS98, BS08]) to protect communications after a quantum computer is built.	Nevertheless, post-quantum public key cryptosystems are being proposed (see e.g. [HPS98, BS08]) to protect communications after a sufficiently strong quantum computer is built.																														
Page 160, Example 3.2.4 last sentence	Then $\varphi_0(\boldsymbol{x}) = 0$.	Then $\varphi_0(0) = 0$.																														
Page 170, first paragraph	which is computationally infeasible according to property (c) of hash functions listed in Sect. 2.1.1.	which is computationally infeasible according to property (b) of hash functions listed in Sect. 2.1.1.																														
Page 177	$m = m_p y_q q + m_q y_p p \bmod n = 2 \times 2 \times 5 + 2 \times 2 \times 3 = 32 \bmod 15 = 2$.	$m = m_p y_q q + m_q y_p p \bmod n = 2 \times 2 \times 5 + 2 \times 2 \times 3 \bmod 15 = 32 \bmod 15 = 2$.																														
Page 209, last paragraph of Section 4.1.1	Similar to SPA, the attack does not require statistical analysis of the traces, only visual inspection is enough.	The sentence should be removed																														