

---

# CRYPTOGRAPHY AND NETWORK SECURITY

## *Errata*

### Chapter 1

<i>Page</i>	<i>Location</i>	<i>Correction</i>
6	Heading 1.3	Change <b>Mechanism</b> to <b>Mechanisms</b>

### Chapter 2

<i>Page</i>	<i>Location</i>	<i>Correction</i>
33	Example 2.17, b	Change <b>34</b> to <b>43</b> .
34	Example 2.19	Change <b><math>(10 \bmod x)^n</math></b> to <b><math>(10 \bmod x)^n \bmod x</math></b>
37	Figure 2.15	Change <b><i>a</i></b> to <b><i>n</i></b>

### Chapter 3

<i>Page</i>	<i>Location</i>	<i>Correction</i>
77	Example 3.18	Change <b>3.22</b> to <b>3.21</b> in the title of the figure
94	Exercise 26	Change <b>"XVIEWYWT"</b> to <b>"XVIEWVWT"</b>

### Chapter 4

<i>Page</i>	<i>Location</i>	<i>Correction</i>
106	Figure 4.6	Change <b>0</b> to <b>1</b> in inverse table (third column, first row) Change <b>1</b> to <b>0</b> in inverse table (third column, second row)

## Chapter 5

<i>Page</i>	<i>Location</i>	<i>Correction</i>
143	Line 9	Change <b>plaintext</b> to <b>encryption cipher</b>
143	Line 10	Change <b>cipher</b> to <b>decryption cipher</b>
153	Line 9	Change <b>cells</b> to <b>taps</b>
153	Line 18	Change $(x^7 + 1)$ to $(x^{15} + 1)$
153	Line 18	Change $(x^3 + 1)$ to $(x^{11} + x^8 + x^7 + x^5 + x^3 + x^2 + x + 1)$
153	Line 18	Change $2^3 - 1 = 7$ to $2^4 - 1 = 15$
164	Table 6.2	Change <b>31</b> to <b>30</b> (the first 31 only)

## Chapter 6

<i>Page</i>	<i>Location</i>	<i>Correction</i>
169	Algorithm 6.1	In the <b>mixer</b> routing, change <b>leftBlock[48]</b> to <b>leftBlock[32]</b> In the <b>mixer</b> routing, change <b>rightBlock[48]</b> to <b>rightBlock[32]</b>
177	Line 8 (3. The...)	Change <b>six</b> to <b>four</b>
188	Exercise 15.a	Change <b>110000</b> to <b>000000</b>
188	Exercise 15.b	Change <b>001111</b> to <b>111111</b>
188	Exercise 23	Change <b>3, 4, and 5</b> to <b>3, 4, 5, and 6</b>

## Chapter 7

<i>Page</i>	<i>Location</i>	<i>Correction</i>
169	Figure 7.4	In the title of the figure, change <b>ciphertext</b> to <b>plaintext</b>
200	Figure 7.8	In matrix X, in the last row, last column, Change <b>0</b> to <b>1</b>
207	Algorithm 7.4	Change $W_{\text{round} + 4c}$ to $W_{4\text{round} + c}$
216	Figure 7.20	At the decryption side, move ( $\leftarrow W_{36} - W_{39}$ ) one sell up
224	Exercise 34	Change <b>MixColumn</b> to <b>MixColumns</b>
224	Exercise 38	Change <b>reverse</b> to <b>inverse</b>

## Chapter 8

<i>Page</i>	<i>Location</i>	<i>Correction</i>
230	Algorithm 8.2	In the title, change <b>ECB</b> to <b>CBC</b>
242	Figure 8.12	Add $x^2$ to the third characteristic

## Chapter 9

Page	Location	Correction
259	Fermat Function	In the shaded area, change $F_1 = 3$ to $F_0 = 3$ In the shaded area, add $F_1 = 5$ above $F_2 = 17$
262	Line 7	Change $a^n - 1$ to $a^{n-1}$
262	Line 8	Change $a^n - 1$ to $a^{n-1}$
271	Example 9.42	Change $15^{(23-1)/2}$ to $16^{(23-1)/2}$
280	Figure 9.7	Change the second (from right) $x_0 = 1$ to $x_1 = 1$

## Chapter 10

Page	Location	Correction
302	Figure 10.6	Remove an extra small <b>2</b> in the encryption box
315	Algorithm 10.6	In the fourth line, change $(q, n)$ to $(p, q)$
316	Algorithm 10.8	In the comment, change the second <b>algorithm</b> to <b>theorem</b>
319	Example 10.10	Delete the word <b>Ciphertext</b> at the beginning of line 5
325	Figure 10.14	Add one extra row to the table Points, <b>(12, 5)</b> <b>(12, 8)</b>

## Chapter 11

Page	Location	Correction
343	Figure 11.6	Remove the word <b>resistance</b> from the title
346	Table 11.3	Add a minus sign in from of the exponent: $P = 1 - e^{-k(k-1)/2N}$
359	Exercise 20	Change <b>(A, B, C, D, E)</b> to <b>(A, B, C, D, F)</b>
361	Exercise 26	Change every <b>m</b> to <b>n</b>
361	Figure 11.16	Change every $\oplus$ to $+$
362	Exercise 27, part i	Change every $+$ to $\oplus$ Change $G_i = H_i \bmod 2^N$ to $G_i = T_i \bmod 2^N$

## Chapter 12

Page	Location	Correction
369	Solution: line 1	Change <b>32</b> to <b>64</b>
371	Table 12.2	In the second column, third row, change last <b>8</b> to <b>B</b>
387	Exercises 20 to 24	Remove extra 4 at the end of the four group <b>(34564</b> to <b>3456)</b>
388	Exercise 32	Remove part b
388	Exercises 34 and 35	Change <b>Figure 12.4</b> to <b>Figure 12.14</b>

## Chapter 13

<i>Page</i>	<i>Location</i>	<i>Correction</i>
394	Figure 13.5	Change <b>Encryption</b> to <b>Decryption</b> in the right box
396	Figure 13.6	Change <b>(M, e, n)</b> to <b>(M, d, n)</b> and change <b>(S, d, n)</b> to <b>(S, e, n)</b>
404	Figure 13.12	In the verifying box, change $M   e_1^{S1} e_2^{-S2}$ to $M   e_1^{S2} e_2^{-S1}$
406	Line 10	Add <b>mod p</b> at the end of the line
410	Line 24	Change $S_{\text{blind}} =$ to $S_b =$
413	Exercise 13	Change <b>h(400)</b> to <b>h (...)</b>

## Chapter 14

<i>Page</i>	<i>Location</i>	<i>Correction</i>
436	Exercise 30	Change <b>second</b> to <b>first</b> at the end of the second line

## Chapter 15

<i>Page</i>	<i>Location</i>	<i>Correction</i>
463	Exercise 12	Change <b>four</b> to <b>two</b>
463	Exercise 15	Change <b>four nonces</b> to <b>two nonces</b>
463	Exercise 15	Change <b>(R<sub>A</sub>, R<sub>B</sub>, R<sub>1</sub>, and R<sub>2</sub>)</b> to <b>(R<sub>A</sub> and R<sub>B</sub>)</b>
463	Exercise 16	Change <b>four nonces</b> to <b>two nonces</b>

## Chapter 16

<i>Page</i>	<i>Location</i>	<i>Correction</i>
489	Figure 16.18	Add <b>Public Key</b> to the lowest box

## Chapter 17

<i>Page</i>	<i>Location</i>	<i>Correction</i>
489	Figure 17.9	Change <b>PM</b> to <b>M</b> (three times)

## Chapter 18

<i>Page</i>	<i>Location</i>	<i>Correction</i>
556	Figure 18.9	Change <b>N + W</b> to <b>N + W + 1</b>
559	Table 18.2	Add <b>Parameters</b> and <b>Description</b> to column heads
565	Figure 18.17	Change $g^y$ and $g^r$

**Chapter 18**

<i>Page</i>	<i>Location</i>	<i>Correction</i>
574	Figure 18.26	Add one padlock to the legend (last item)
591	Exercise 19	Change <b>19</b> to <b>18</b>
591	Exercise 30	Change <b>general</b> to <b>original</b>
592	Exercise 36	Change <b>36</b> to <b>35</b>

