CRYPTOGRAPHY AND NETWORK SECURITY

Errata

Chapter 1

Page	*Location*	*Correction*
6	Heading 1.3	Change **Mechanism** to **Mechanisms**

Chapter 2

Page	*Location*	*Correction*
22	Divisibility	Change **a|n to n|a. The same with *a* not divide *n*.**
33	Example 2.17, b	Change **34** to **43.**
34	Example 2.19	Change **$(10 \bmod x)^n$** to **$(10 \bmod x)^n \bmod x$**
37	Figure 2.15	Change ***a*** to **n**

Chapter 3

Page	*Location*	*Correction*
77	Example 3.18	Change **3.22 to 3.21** in the title of the figure
94	Exercise 26	Change **"XVIEWYWT"** to **"XVIEWVWT"**

Chapter 4

Page	*Location*	*Correction*
106	Figure 4.6	Change **0 to 1** in inverse table (third column, first row) Change **1 to 0** in inverse table (third column, second row)

Chapter 5

Page	Location	Correction
143	Line 9	Change **plaintext** to **encryption cipher**
143	Line 10	Change **cipher** to **decryption cipher**
153	Line 9	Change **cells** to **taps**
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 **31** to **30** (the first 31 only)

Chapter 6

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

Chapter 7

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

Chapter 8

Page	Location	Correction
230	Algorithm 8.2	In the title, change **ECB** to **CBC**
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 **2** 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 **algorithm** to **theorem**
319	Example 10.10	Delete the word **Ciphertext** at the beginning of line 5
325	Figure 10.14	Add one extra row to the table Points, **(12, 5) (12, 8)**

Chapter 11

Page	*Location*	*Correction*
343	Figure 11.6	Remove the word **resistance** 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 **(A, B, C, D, E)** to **(A, B, C, D, F)**
361	Exercise 26	Change every **m** to **n**
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 **32** to **64**
371	Table 12.2	In the second column, third row, change last **8** to **B**
387	Exercises 20 to 24	Remove extra 4 at the end of the four group (**34564** to **3456)**
388	Exercise 32	Remove part b
388	Exercises 34 and 35	Change **Figure 12.4** to **Figure 12.14**

Chapter 13

Page	Location	Correction
394	Figure 13.5	Change **Encryption** to **Decryption** in the right box
396	Figure 13.6	Change **(M, e, n)** to **(M, d, n)** and change **(S, d, n)** to **(S, e, n)**
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 **mod *p*** at the end of the line
410	Line 24	Change **S_{blind} =** to **S_b =**
413	Exercise 13	Change **h(400)** to **h (...)**

Chapter 14

Page	Location	Correction
436	Exercise 30	Change **second** to **first** at the end of the second line

Chapter 15

Page	Location	Correction
463	Exercise 12	Change **four** to **two**
463	Exercise 15	Change **four nonces** to **two nonces**
463	Exercise 15	Change **(R_A, R_B, R_1, and R_2)** to **(R_A and R_B)**
463	Exercise 16	Change **four nonces** to **two nonces**

Chapter 16

Page	Location	Correction
489	Figure 16.18	Add **Public Key** to the lowest box

Chapter 17

Page	Location	Correction
489	Figure 17.9	Change **PM** to **M** (three times)

Chapter 18

Page	Location	Correction
556	Figure 18.9	Change **N + W** to **N + W + 1**
559	Table 18.2	Add **Parameters** and **Description** to column heads
565	Figure 18.17	Change g^y and g^r

Chapter 18

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