Errata List 06.06.2014

Chapter	Page	Section	
1	15	1.4.1	"9|(21-3)" should be "9|(12-21)", "9|(-6-3)" should be "9|(12-(-6))"
1	17	1.4.2	In line 5: Addition and multiplication are associative, e.g. -> "e.g." should be replaced by "i.e."
1	17	1.4.2	One bullet point is missing here: "Addition is commutative, e.g., $a + b = b + a$, for all $a,b,\in \mathbb{Z}_m $."
2	40	2.2.1	It should state mod 2 instead of mod m
3	43	2.3	In the whole figure it should be s0 <-> s1 and p0 <-> p1
2	45	2.3.1	In Tab. 2.3, (0,1,3,4,8) is not a primitive polynom
2	47	2.3.3	In Fig. 2.8, the output of the AND gate should NOT be added to the key stream. It should only be added to the input of the next LFSR
2	52	Problem 2.1	Last character of the ciphertext should be 'r' instead of 'p'
2	52	Problem 2.5	c_2, c_1, c_0 should be replaced by p_2, p_1, p_0
3	73	3.4	First line beneath Definition 3.5.1 should be 1/2^8, not 1/2^16 (see Theorem 5.2.1 on p.137)
4	92	Def. 4.3.2	Replace "additive group" by "additive abelian group", and "multiplicative group" by "multiplicative abelian group"
4	114	4.5	The inverse affine transformation should be $\begin{pmatrix} b'_0 \\ b'_1 \\ b'_2 \\ b'_3 \\ b'_4 \\ b'_5 \\ b'_6 \\ b'_7 \end{pmatrix} \equiv \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$
4	116	4.7	Third line from the bottom: Change 50Mbit/s to 50Gbit/s
4	119	Problem 4.9	Change the second sentence to "[...] if the input of the first Byte Substitution Layer consists of 128 ones, and the second subkey (i.e., k_1) also consists of 128 ones?"
5	126	5.1.1	Replace "Note that bank B now has means of ..." by "Note that bank B has no means of ..."
5	133	5.1.5	We are assuming a 128 bit block cipher, there are 16 bytes in each block. Thus, there should be 16 x 2^32 = 2^36 bytes that can be encrypted under this IV.
5	135/136	5.1.6	In the description of Fig. 5.8, ADD should be replaced by AAD
5	139	5.3.1	The first formula in Phase II should be y1, not x1
5	146	Problem 5.10	In Point 5., "specific bit errors" are bit errors that occur at the same position(s) as the original bit error(s)
6	164	6.3.2	"addition and multiplication are the same operations" should be "addition and subtraction are the same operations"
7	185	7.5.2	In the first step of Example 7.6, the second y_p should be changed to y_q
7	191	7.6.2	In the Miller-Rabin Primality Test, the loop 1.4 should be left if the equation z = p-1 is fulfilled
7	195	7.8	The column by Martin Gardner was published in 1977
8	219	8.3.2	In point 4, "...generalization as elliptic curves" should be replaced to "...generalization of elliptic curves"
8	228	8.5.2	In the protocol, k_{pub} in one of Bob's computations "k_{pub} = \beta..." should be deleted
8	229	8.5.3	In the second line of "Key Generation" the word "key" is missing: "...and the public and private key have to be computed."
8	231	8.5.4	In line 11 of subsection "Active Attacks", Alice sends the two ciphertexts (y_1, k_E) and (y_2, k_E) over the channel
8	234	Problem 8.3	The groups that should be studied here are from Problem 8.1
8	237	Problem 8.17	Reference to 8.13 not correct. Sentence should state "A given plaintext has many valid ciphertexts."
9	256	9.2	(2,7), (5,2) and (3,6) are not on the elliptic curve
10	259	10	Line 1: "...cryptographic tools they and are" - should be "...and they are"
10	266	10.2.1	In line 9, "...RSA encryption requires..." should be "...RSA decryption requires..."
10	271	10.3.1	Elgamal Signature Generation: k_E is chosen randomly from 2 to p-2
10	274	10.3.3	First sentence of "Reuse of the Ephemeral Key": It should be private key d instead of a
10	291	Problem 10.13	Due to the definition of k_E, there are no consecutive k_E that can fulfill this equation
11	307	11.4	In the third line from the bottom, the maximum length of a SHA-1 input is limited by 2^{64}-1
12	322	12.2	In the attack against secret prefix MACs, "valid signature" should be changed to "valid MAC"
12	325	12.2	In the middle of the page: "The hash output length l is in practice longer" should be replaced by "... is in practice shorter"
13	342	13.3	In line 5: "For the former" should be "For the latter"
13	344	13.3.1	2nd line of Oscar's operation in Box should be "decrypt x = AES^{-1}_{kAO} (y)"
13	345	13.3.2	Line 5 should state "The problem of trusted distribution of public keys is central in modern public-key cryptography"
13	346	13.3.2	DHKE with Certificates (Bob): \alpha^B should be replaced by \alpha^b
13	349	13.3.3	In line 9: "... private keys of all these different CAs ..." - "private" should be replaced by "public"
13	350	13.3.3	In line 5, the letter 'e' in "signes" should be deleted
References	359	[12]	"2999" should be replaced by "2000"