Errata List		28.03.2019		
Chapter	**Page**	**Section**	**Figure**	**Comment**
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		"Addition and multiplication are \emph{associative}, e.g." -> e.g. should be i.e.
1	17	1.4.2		add bulletpoint "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
2	43		2.7	In the whole figure it should be s0 <-> s1 and p0 <-> p1 and FF0 <-> FF1
2	45	2.3.1	Tab. 2.3	(0,1,3,4,8) is not a primitive polynom
2	47	2.3.3	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	50	Problem 2.1		The last letter of the cipher text should be a "r", not a "p"
2	52	Problem 2.5		c_2, c_1, c_0 should be replaced by p_2, p_1, p_0
3	73	3.5.1		First line beneath Definition 3.5.1 should be 1/2^8, not 1/2^16 (see Theorem 5.2.1, p.137)
4	91			the last line contains two successive a's
4	92	Def. 4.3.2		replace "additive group" -> "additive abelian group", and "multiplicative group" -> "multiplicative abelian group"
4	97	4.3.5		"We need irreducible polynomials for the module reduction [...]" should be "We need irreducible polynomials for the modulo reducti
4	107	4.4.4		THe W equations use + when they should be XOR.
4	114	4.5		The inverse affine transformation should be $\begin{pmatrix} b'_0 \\ b'_1 \\ b'_2 \\ b'_3 \\ b'_4 \\ b'_5 \\ b'_6 \\ b'_7 \end{pmatrix} = \begin{pmatrix} 0&0&1&0&0&1&0&1 \\ 1&0&0&1&0&0&1&0 \\ 0&1&0&0&1&0&0&1 \\ 1&0&1&0&0&1&0&0 \\ 0&1&0&1&0&0&1&0 \\ 0&0&1&0&1&0&0&1 \\ 1&0&0&1&0&1&0&0 \\ 0&1&0&0&1&0&1&0 \end{pmatrix} \begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$
4	116	4.7		50Mbit/s should be 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	124	5.1		The ECB and CFB modes require -> The ECB and CBC modes require
5	126	5.1.1	-	Replace "Note that bank B now has means of detecting..." by "Note that bank B has no means of detecting...".
5	131	5.1.3	5.5	e^(-1) should be e on the receiver side
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	133			8bytes is incorrect -> "Since every block consists of 16 bytes, a maximum of 16×232 = 2^36 bytes, or about 64 Gigabytes"
5	134	5.1.6		"as the XOR sum of the current ciphertext y_i and g_i" -> "as the XOR sum of the current ciphertext y_i and g_{i-1}
5	135	5.1.6	-	a few times: AAD instead of ADD
5	139	5.3.1		The first formula in Phase II should be y1, not x1
5	139	5.3.1	-	"If it is *not* in the table, we increment the key to *kR*,1" -> "If it is not in the table, we increment the key to kR,2"
5	142		-	Def. 5.3.1, decryption: replace e−1k,k1,k2(x) by e−1k,k1,k2(y)
5	146	Problem 5.10	-	specific bit errors: bit errors at the same position(s) as the original bit error(s)
6	164	6.3.2		"addition and multiplication are the same operations" -> "addition and subtraction are the same operations"
7	184			exponentiation x^d mod n efficiently. -> exponentiation y^d mod n efficiently. x_p ≡ x mod p -> y_p ≡ y mod p x_q ≡ x mod q -> y_q ≡ y mod q y_p = x_p^{d_p} mod p -> x_p = y_p^{d_p} mod p y_q = x_q^{d_q} mod q -> x_q = y_q^{d_q} mod q y ≡ [q c_p] y_p + [p c_q] y_q mod n -> x ≡ [q c_p] x_p + [p c_q] x_q mod n
7	185	7.5.2	-	In the example: replace 2nd y_p with y_q
7	186	Fermat-Test		Step 1.2: change line to: IF $a^{\tilde{p}-1} \not\equiv 1$ \bmod \tilde{p}
7	191	MR-Alg	-	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		Columne by Martin Gardner war written in 1977, not in 1997
8	209	8.2.1	-	a^-1 = (u-i*v)/(u^2+v^2) (v is missing)
8	210	8.2.1		Theorem 8.2.1.: Since i=0 has no inverse, i=1, ..., n-1 with gcd(i,n)=1
8	219	8.3.2	-	4. ...generalization OF elliptic curves
	226	8.4	-	"Hence, the smalles prime factor of p-1..." should be "Hence, the largest prime factor of p-1..."
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	-	Key Generation ...and the public and private KEY have to ...
8	231	8.5.4	-	She would send the two ciphertexts (y1, kE) and (y1, kE) over the channel. <- y2
8	231	8.5.4		"Just as in the DHKE protocol, we have to be careful that we do not fall vicitim [...]" -> should be "[...] victim [...]".
	232	8.6	-	"Z_p" should be "Z_p*"
8	232	8.6	-	"Tahar" replace by "Taher"
8	233	8.7	-	"Z_p" should be "Z_p*"
8	237	Problem 8.17	-	Reference to 8.13 not correct. Sentence should state "A given plaintext has many valid ciphertexts."
8	237	Problem 8.18		Problem 8.18, he correct ciphertexts are (3, 15),(19, 14),(6, 15),(1, 4),(22, 13),(4, 7),(13, 4),(3, 21),(18, 17),(26, 25),(7, 17)
9	241			(cf. Sect. 4.2) -> (cf. Sect. 4.3)
9	253	9.5	-	"that only generic attacks (c.f. Sect. 8.3.3) are know ECC" replace by "that only generic attacks (c.f. Sect. 8.3.3) are known for ECC"
9	256	Problem 9.2	-	(2,7), (5,2) and (3,6) are not on the elliptic curve, Fix: 1. (13,7)+(6,3) ; 2. (13,7)+(13,7) , y^2 =x^3 +2x +3 mod 17, Answers:(7,11),(10,11)
10	259	10		Line 1: "...cryptographic tools they and are" - should be "...and they are"
10	263	10.1		In the figure, the verification must be done with kpub,B not kpr,B
10	265			"yielding x" replace by "yielding x'
10	266	10.2.1		Line 9: "...RSA encryption requires..." should be "...RSA decryption requires..."
10	269	10.2		"[...] and the role the play [...]" should be "[...] and the role they play [...]"
10	269	10.2.3		In point 5 it should state: "Apply a mask generation function MGF to the hash of string M' [...]"
10	271	10.3.1	-	2.Box: k_E ranges from 2,3,...,p-2
10	274	10.3.3	-	First sentence of "Reuse of the Ephemeral Key": " It should be private key d" (i.e., replace "a" with "d"
10	291	Excercise 10.13	-	There are not valid k_E that fulfill the condition
11	307	11.4	-	maximum length for SHA-1 input is 2^{64}-1
12	322	12.2		More specific/ clear: The key will be appended with zeroed bytes from the LSB side
12	322	12.2	Protokoll	in protocol "box": "valid signature" -> "valid checksum"
12	325	12.2	-	"output length l is in practice longer" replace by "output length l is in practice shorter"
13	342		-	l. 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)" not "decrypt x = AES^-1_kAO (x)"
13	345	13.3.2	-	Line 5 should state "The problem of trusted distribution of public keys is central in modern public-key cryptography", not "private keys is central..."

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		... Where each CA signEs...
13	353			Problem 13.3.: Change last sentence to "Justify your answer."
13	354	Problem 13.5		replace "all recent keys $e_{k^{(i)}_{U,KDC}}$" by "all recent keys $k^{(i)}_{U,KDC}$"
13	357	Problem 13.18		replace $k_{pr, CA}$ with $k_{pub, CA}$
References	359	[12]		"2999" should be "2000"