

TYPOS TO BE CORRECTED IN THE FOURTH PRINTING OF INTRO to CRYPTO

PAGE NUMBER	LINE NUMBER	MISPRINT → CORRECTION
4	Footnote 1.11, line 3	<i>They hung flags</i> → <i>They flung hags</i>
4	Footnote 1.11, line 5	<i>They flung hags</i> → <i>They hung flags</i>
25	11	Then → then
38	13	$-b \leq a_0 \rightarrow -b < a_0$
39	-4	, → ,
46	Exercise 1.76	$(1, 1) \rightarrow (11)$
49	22	$(\ln n)(\ln \ln n) \rightarrow \ln \ln n$
69	10	$m_j \geq 1$ of $r_j \rightarrow m_j \geq 1$ of n_j
80	-2	<i>MGXAJ</i> → <i>MGXXAJ</i>
83	-8 (above footnote)	$A \rightarrow e$
84	-12	$(7, 19) \rightarrow (1, 23)$
85	8	$D_d = D_{e^{-1}} \rightarrow D_d(c) = D_{e^{-1}}(c)$
122	-6 (above footnote)	$b = (100011110101100) \rightarrow b = (001101011110001)$
126	Exercise 2.56	$(c_0, c_1, c_2, c_3) = (1, 0, 0, 1) \rightarrow (c_1, c_2, c_3, c_4, c_5) = (1, 0, 0, 1, 0)$
132	8	$\alpha^{(p-1)b_0/p_j} \rightarrow \alpha^{(p-1)b_0^{(j)}/p_j}$
139	12	roots of → roots
140	-12	$n = 1493 \rightarrow 1943$
145	17	$q \equiv 3 \pmod{pq} \rightarrow q \equiv 3 \pmod{4}$
158	7	$= r(x)$, which → , which
161	-2	$e \Rightarrow d =$
164	-4 (above footnote)	$r(t) \rightarrow r(e)$
166	Example 4.13	$\text{ind}_2^{29}(5) \equiv 22 \pmod{29} \rightarrow \text{ind}_2^{29}(5) = 22$
170	5	$\phi(n)/g \rightarrow \phi(p^c)/g$
175	-2 (above footnote)	$(\frac{b}{n}) \rightarrow (\frac{a}{n})$
190	Example 4.66	$a \in \{1, 3\} \rightarrow a \in \{3\}$,
190	-6 above footnote	$t \in \mathbb{N} \rightarrow t \in \mathbb{N}, n$ is composite
190	-3, -4 above footnote	, and n is composite, → ,
190	-2 above footnote	for composite n , → ,
191	-4 above footnote	$j \geq 1 \rightarrow j \geq 0$
259	2	$H \rightarrow G$
299	-1 (above footnote)	$k \in \mathbb{N} \rightarrow k$
301	9	if otherwise → otherwise
314	Exercise 2.55	$b = (000111101011001) \rightarrow b = (100110101111000)$

Thanks go to Robert F. Morse and his cryptography class who pointed out several of the above on March 5, 2002. They also noted that it would be more appropriate for Footnote 2.31 on page 106 to be put at the end of the third paragraph.

Table 1.4 on page 17 needs a fix. In rows 2–3 (under the row of numbers) replace VA by AX (once for each row).

Questions by one of my current students, Kjell Wooding, led to the following. The complete description of *ones' complement* on pages 35–36 has to be replaced. Delete everything from line -3 (above the footnotes on page 35 starting with: “Let $(a_{t_n} a_{t_n-1} \dots a_0) \dots$ ” to line 10 on page 36 ending with: “... represented by $(01)_2$.” by the following.

If $n \in \mathbb{Z}$ and $(|n|)_{10} = (a_{t_n} a_{t_n-1} \dots a_0)_2$, then for any integer $m > t_n + 1$, the *ones' complement* m -bit representation of n is given by:

$$\begin{cases} \underbrace{(00 \dots 0}_{m-t_n-1 \text{ copies}} a_{t_n} a_{t_n-1} \dots a_0)_2 & \text{if } n > 0, \\ \underbrace{(11 \dots 1}_{m-t_n-1 \text{ copies}} 1 - a_{t_n} 1 - a_{t_n-1} \dots 1 - a_0)_2 & \text{if } n < 0, \end{cases}$$

The $n \in \mathbb{Z}$ which can be represented as m -bit ones' complement binary integers are those in the range $-2^{m-1} - 1 \leq n \leq 2^{m-1} - 1$. The basic idea is to convert n to a binary digit and pack $m - t_n - 1$ zeros to the left. Then if $n > 0$, this is the ones' complement, whereas if $n < 0$, then replace all zeros by ones and all ones by zeros. This is illustrated as follows.

Example 1.12 To represent $(26)_{10}$ and $(-26)_{10}$ as $m = 7$ -bit ones' complement integers, we calculate that $(26)_{10} = (11010)_2$, so $(0011010)_2$ is the 7-bit ones' complement representation of the decimal digit 26, whereas for -26 it is $(1100101)_2$. See Exercises 1.39–1.40 on page 43.

Notice that in the ones' complement system, $+0$ is represented by $(00)_2$, as an $m = 2$ -bit binary integer, and -0 is represented by $(11)_2$.

On page 43, change the initial statement in Exercise 1.39 to read:

Provide the 7-bit ones' complement representation of each of the following. Then change the solution on page 308 to read:

- (a) $(1110101)_2$ (b) $(1101010)_2$ (c) $(0011110)_2$ (d) $(0100001)_2$

As pointed out to me by my colleague, Norbert Sauer, here at U of C, the proof of Theorem 2.17 on page 64 needs to be reformulated. Replace the proof by the following:

If $p \mid n$ is a prime and $p < n$, then $p \mid (n - 1)!$. Thus, given that $(n - 1)! \equiv -1 \pmod{n}$, we have

$$0 \equiv (n - 1)! \equiv -1 \pmod{p},$$

a contradiction.

On pages 93–94, the data in Example 2.49 should be replaced by the following from the first matrix on page 93 up to the middle of page 94 where we have "Hence,...":

1	2	3	4	5	6	7
9	10	11	12	13	14	15
17	18	19	20	21	22	23
25	26	27	28	29	30	31
33	34	35	36	37	38	39
41	42	43	44	45	46	47
49	50	51	52	53	54	55
57	58	59	60	61	62	63

↓ PC1

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

Let the input key be $k = (e_1 e_2 \dots e_7, e_9, \dots, e_{62}, e_{63}) =$

$$(1100011110000100010111110101011100011010101111100011110).$$

The following illustrates the effect of **PC1** on k , where we list the key and the output as a 2×56 array with the first row being the position for the sake of increased clarity.

		k															
j		1	2	3	4	5	6	7	9	10	11	12	13	14	15	17	18
e_j		1	1	0	0	0	1	1	1	1	0	0	0	0	1	0	0

j		19	20	21	22	23	25	26	27	28	29	30	31	33	34
e_j		0	1	0	1	1	1	1	1	0	1	0	1	0	1

j		35	36	37	38	39	41	42	43	44	45	46	47	49	50
e_j		1	1	0	0	0	1	1	0	1	0	1	0	1	1

j		51	52	53	54	55	57	58	59	60	61	62	63
e_j		1	1	1	1	0	0	0	1	1	1	1	0

		PC1 (k)															
j		1	2	3	4	5	6	7	9	10	11	12	13	14	15	17	18
$e_{\mathbf{PC1}(j)}$		0	1	1	0	1	0	1	1	0	1	1	1	1	0	1	1

j		19	20	21	22	23	25	26	27	28	29	30	31	33	34
$e_{\mathbf{PC1}(j)}$		1	1	0	1	1	0	0	0	1	1	1	1	0	0

j		35	36	37	38	39	41	42	43	44	45	46	47	49	50
$e_{\mathbf{PC1}(j)}$		0	0	1	1	1	1	1	1	1	0	0	1	0	1

j		51	52	53	54	55	57	58	59	60	61	62	63
$e_{\mathbf{PC1}(j)}$		1	1	0	0	1	0	0	0	0	1	0	0

For instance, $\mathbf{PC1}(1) = 57$, so

$$e_{\mathbf{PC1}(1)} = e_{57} = 0$$

under the action of the permutation **PC1**, and this is the first bit in the permuted key. Similarly, $\mathbf{PC1}(20) = 51$, so

$$e_{\mathbf{PC1}(20)} = e_{51} = 1$$

is the bit in position 20 of the permuted key.

at the bottom of the page, the entry in the right **PC2** matrix in position row 6, column 4, the 44 should be replaced by a 45.

On page 140, lines 3 to 11 must be replaced by the following.

2-digit, base 26 integer: **EX**= $4 \cdot 26 + 23 = 127$; **AM**= $0 \cdot 26 + 12 = 12$; **SA**= $18 \cdot 26 + 0 = 468$; **RE**= $17 \cdot 26 + 4 = 446$; **HA**= $7 \cdot 26 + 0 = 182$; **RD**= $17 \cdot 26 + 3 = 445$. Thus,

$$\mathcal{M} = \{127, 12, 468, 446, 182, 445\}.$$

Then we encipher each block via $m^{701} \equiv c \pmod{1943}$ to get,

$$\mathcal{C} = \{1461, 1926, 468, 11, 1371, 271\},$$

each of which is written as a 3-digit, base 26 integer: $1461 = 2 \cdot 26^2 + 4 \cdot 26 + 5 = \mathbf{CEF}$; $1926 = 2 \cdot 26^2 + 22 \cdot 26 + 2 = \mathbf{CWC}$; $468 = 0 \cdot 26^2 + 18 \cdot 26 + 0 = \mathbf{ASA}$; $11 = 0 \cdot 26^2 + 0 \cdot 26 + 11 = \mathbf{AAL}$; $1371 = 2 \cdot 26^2 + 0 \cdot 26 + 19 = \mathbf{CAT}$; $271 = 0 \cdot 26^2 + 10 \cdot 26 + 11 = \mathbf{AKL}$. Then the cryptogram is sent as: **CEFCWCASAAALCATAKL**. The receiver may then decipher using $c^{29} \equiv m \pmod{1943}$ after converting the letters to 3-digit base 26 numerical equivalents. For instance, $1461^{29} \equiv 127 \pmod{1943}$.

On page 156, add the comment just before the statement of the Chor-Rivest knapsack cipher:

Until recently the following was the only known secure knapsack cipher. However, it was broken by S. Vaudenay (see J. Cryptology (2001), 87–100).

As a consequence, also delete the first sentence of the first complete paragraph on page 159.

In Example 4.6 on page 162, 6 is not a primitive root modulo 1777. This requires the replacement of $\text{ord}_{1777}(6) = 1776$ by $\text{ord}_{1777}(5) = 1776$, followed by the comment that 5 is a primitive root modulo 1777. Since this is based upon the same error in Example 3.15 on page 143, this requires replacing that example with the following:

Example 3.15 Let $p = 1777$ and choose a generator $\alpha = 5$ of \mathbb{F}_{1777}^* . Entity B chooses a private key $a = 146$, and computes

$$\alpha^a = 5^{146} \equiv 1729 \pmod{p}.$$

Thus, B 's public key is $(p, \alpha, \alpha^a) = (1777, 5, 1729)$, which A gets from a public file. To encipher $m = 1483$, say, A selects $b = 1066$ randomly and computes

$$\beta = 5^{1066} \equiv 1664 \pmod{1777},$$

and

$$\gamma \equiv 1483 \cdot 1729^{1066} \equiv 625 \pmod{1777}.$$

Then A sends $(\beta, \gamma) = (1664, 625)$ to B . To decipher, B computes

$$\beta^{p-1-a} = 1664^{1777-1-146} \equiv 1768 \pmod{1777},$$

and recovers m by computing

$$m = \beta^{-a} \gamma \equiv 1768 \cdot 625 \equiv 1483 \pmod{1777}.$$

Thanks go to David Feldman of the University of New Hampshire for pointing out the following problems.

On page 221, replace lines 15–20 of Section 6.1, beginning with “Basically, what Wiles did...” and ending with “...to prove it.” with the following:

The means by which this was accomplished (in the last twenty years of the history of FLT) began with a 1982 conjecture posed by Gerhard Frey that a solution to the Fermat Equation (given in Footnote 1.40 on page 22) would imply the existence of an elliptic curve which is *semi-stable* but not *modular* (see [162]). This conjecture was proved in 1986 by Ken Ribet. In 1993, Wiles claimed to have a proof that all semi-stable elliptic curves with rational coefficients are modular. However, his proof had holes in it. With the aid of Richard Taylor, these gaps were plugged by early 1995. Hence, FLT fell to the contradiction after centuries of attempts to prove it.

My former student, now cryptographer at CSE, Gary Walsh, who is also teaching a cryptography course from the text at the University of Ottawa, noted that the enciphering stage (2) of the ElGamal Public-Key Elliptic Curve Cryptosystem needs to be changed to reflect the fact that message units must be points on the curve, as indeed is illustrated in Example 6.36 after the description of the cryptosystem on page 244. I think that this is best done as follows. Alter (2) to read:

(2) Consider the plaintext message units embedded as points m on E .

Definition A.5 on page 272 requires a correction. Replace the last five sentences on page 272 (those lines after the displayed set $\mathcal{S} \times \mathcal{T} = \{(s, t) : s \in \mathcal{S}, t \in \mathcal{T}\}$) by the following:

A relation R on $\mathcal{S} \times \mathcal{T}$ is a subset of $\mathcal{S} \times \mathcal{T}$ where $(s, t) \in R$ is denoted by sRt . A relation on $\mathcal{S} \times \mathcal{S}$ is called a binary relation. A relation R on $(\mathcal{S} \times \mathcal{S}) \times \mathcal{S}$ is called a binary operation on \mathcal{S} if R associates with each $(s_1, s_2) \in \mathcal{S} \times \mathcal{S}$, a unique element $s_3 \in \mathcal{S}$. In other words, if $(s_1, s_2)Rs_3$ and $(s_1, s_2)Rs_4$, then $s_3 = s_4$.

Also, on the first line of page 273, replace $\{(1, 2), (1, 3)\}$ with $\{(1, 1), (1, 2)\}$.

Replace Definition A.6 on page 273 by the following:

Definition A.6 (Functions)

A *function* f (also called a *mapping* or *map*) from a set \mathcal{S} to a set \mathcal{T} is a relation on $\mathcal{S} \times \mathcal{T}$, denoted by $f : \mathcal{S} \rightarrow \mathcal{T}$, which assigns each $s \in \mathcal{S}$ a unique $t \in \mathcal{T}$, called the *image of s under f* , denoted by $f(s) = t$. The set \mathcal{S} is called the *domain* of f and \mathcal{T} is called the *range* of f . If $\mathcal{S}_1 \subseteq \mathcal{S}$, then the *image of \mathcal{S}_1 under f* , denoted by $f(\mathcal{S}_1)$, is the set

$$\{t \in \mathcal{T} : t = f(s) \text{ for some } s \in \mathcal{S}_1\}.$$

If $\mathcal{S} = \mathcal{S}_1$, then $f(\mathcal{S})$ is called the *image of f* , denoted by $\text{img}(\mathcal{S})$. If $\mathcal{T}_1 \subseteq \mathcal{T}$, the *inverse image of \mathcal{T}_1 under f* , denoted by $f^{-1}(\mathcal{T}_1)$, is the set

$$\{s \in \mathcal{S} : f(s) \in \mathcal{T}_1\}.$$

A function $f : \mathcal{S} \rightarrow \mathcal{T}$ is called *injective* (also called *one-to-one*) if and only if for each $s_1, s_2 \in \mathcal{S}$, $f(s_1) = f(s_2)$ implies that $s_1 = s_2$. A function f is *surjective* (also called *onto*) if $f(\mathcal{S}) = \mathcal{T}$, namely if for each $t \in \mathcal{T}$, $t = f(s)$ for some $s \in \mathcal{S}$. A function f is called *bijective* (or a *bijection*) if it is both injective and surjective. Two sets are said to be in a *one-to-one correspondence* if there exists a bijection between them.

After the above replacement of the definition, add the following for further clarification.

Each of the following may be verified for a given function $f : \mathcal{S} \rightarrow \mathcal{T}$.

1. If $\mathcal{S}_1 \subseteq \mathcal{S}$, then $\mathcal{S}_1 \subseteq f^{-1}(f(\mathcal{S}_1))$.
2. If $\mathcal{T}_1 \subseteq \mathcal{T}$, then $f(f^{-1}(\mathcal{T}_1)) \subseteq \mathcal{T}_1$.
3. The identity map, $1_{\mathcal{S}} : \mathcal{S} \rightarrow \mathcal{S}$, given by $1_{\mathcal{S}}(s) = s$ for all $s \in \mathcal{S}$, is a bijection.
4. f is injective if and only if there exists a function $g : \mathcal{T} \rightarrow \mathcal{S}$ such that $gf = 1_{\mathcal{S}}$, and g is called a *left inverse of f* .
5. f is surjective if and only if there exists a function $h : \mathcal{T} \rightarrow \mathcal{S}$ such that $fh = 1_{\mathcal{T}}$, and h is called a *right inverse for f* .
6. If f has both a left inverse g and a right inverse h , then $g = h$ is a unique map called the *two-sided inverse of f* .
7. f is bijective if and only if f has a two-sided inverse.

Thanks also go to some of my current students in PMAT 321 at U of C this term, (Fall 2001), for pointing out some of the above typos:

Mike Burrell, Richard Burton, Chris Foster, Christine Machacek, Rob Pearson, Bill Rosgen, and Stephanie Staite.