Errata for Introduction to Cryptography with Coding Theory, 2nd edition

by Wade Trappe and Lawrence C. Washington

page 20, line 3: "ciphertext" should be "plaintext"

page 22 line 10: Exercise 9 should be Exercise 12.

page 24, line 5: insert "the" before "largest"

page 24, line 19: change "For $j = 1$ to 25" to "For $j = 0$ to 25"

page 42, lines 21-24: **Comment:** Since a one-way function could have constant last bit, this method might not yield a pseudo-random sequence. However, in practice it works well. How is the random seed s chosen? Keystrokes, clock timings, and things like that are often used to produce seeds.

page 49, line -15: the congruence should be $b_m x_{n+m} \equiv -x_{n+m}$

page 49, line -14: The displayed equivalence should be

$$x_{n+m} \equiv b_0 x_n + b_1 x_{n+1} + \cdots + b_{m-1} x_{n+m-1}$$

page 49, line -13: the line should read "This is a recurrence of length m. Since $m \leq N - 1$ and N is assumed to"

page 50, end of section 2.11: add "Also, several LFSRs can be combined nonlinearly and some of these LFSRs can have irregular clocking."

page 58, Problem 25: change part (a) to "What property of the ciphertext will make Eve suspect that the plaintext is a string of one, two, three, or six letters repeated several times and will allow her to guess that the key length is six?"

page 59, line 1: change "recognizes" to "guesses"

page 60, Problem 8: the ciphertext should end in the middle of the next to last line with `weiuk`. Remove `mvswr...vbel`, which seems to have migrated from the second line of the the ciphertext of Problem 7.

page 64, line 14: The sentence should read "A number $p > 1$ whose only positive divisors are 1 and itself is called a **prime number**."

page 69, line -12: change this line to "have calculated $x_{n+1} = -590$, which, up to sign, is the original number 1180 divided by"

page 70, line -9: change "positive or negative" to "positive, negative, or zero"

page 75, line -8: change 6713 (mod 12345) to 6173 (mod 12345)

page 83, line -9: change "(p)" to "$(\bmod\ p - 1)$"

page 84, line -6: change $(p-1)r$ to $(p-1)q$

page 91, Theorem, part 4: change " $(\bmod\ n)$" to " $(\bmod\ 8)$" (twice)

page 91, line -13: change "$(-1)^{(n-1)/2}$" to "$a^{(n-1)/2}$"

page 114, lines 5-7, and page 123, lines 12-14: **Comment:** Biham and Shamir have published a differential cryptanalytic attack that beats exhaustive key search on the full 16 round DES

page 123, line -16: change "A block of ciphertext" to "A block of plaintext"

page 123, line -14: remove the space between 1s and the period.

page 129, lines 12-13: change "differ by 2 bits" to "differ by at least 2 bits"

page 134, Figure 4.7: O_1 and O_2 in the gray shading at the top of the diagram (corresponding to the 8 rightmost bits of X_2 and X_3) should be C_1 and C_2.

page 134, last displayed equation: It should be "R_{56}" and "R_{48}".

page 149, line 2: change "c_1" to "C_1"

page 152: **Comment:** After Rijndael was selected to become the AES, the NIST editor of the FIPS document specifying AES decided to change the names of the layers. The official names are now SubBytes, ShiftRows, MixColumns and AddRoundKey

page 158, line -5: change "**InvByteSub**" in step 2 to "**InvShiftRow**" (or to "**InvShiftRows**")

page 162, Exercise 1(a): the top line of the matrix should be 01100010 (not 01100100)

page 162, Problem 2(a): the values of $W(4) = W(6)$ and $W(5) = W(7)$ are switched.

page 171. line 11: change "if" to "of"

page 184, line -5: change "then $\gcd(x - y, n) = 1$ or n" to "then usually $\gcd(x - y, n) = 1$ or n"

page 192, problem 2(a): change "decryption modulus" to "decryption exponent"

page 192, problem 6: change $(\bmod\ p)$ to $(\bmod\ n)$ (3 times)

page 193, problem 13: "Explain what the steps you would do" should be "Explain what steps you would do"

page 195, Exercise 23: For simplicity, assume $\gcd(12345, e) = 1$.

page 196, line 7: change 2703000 to 270300

page 209, line 17: change "$(\bmod\ p)$ let" to "$(\bmod\ p)$. Let"

page 211, line -2: change "β" to c

page 216: Exercise 12(a): assume $\gcd(c, n) = 1$ (otherwise the second list cannot be computed)

page 220, line -5: change "Exercise 9" to "Exercise 7"

page 222, lines 4-5: change "a function" to "an algorithm"

page 231, line 8: change "probability is" to "probability is approximately"

page 231, line 9: change $\lambda^i e^{-\lambda}/i!$ to "approximately $\lambda^i e^{-\lambda}/i!$"

page 234, line -13: change $n_2 n_1 2^{n_1/2}$ to $\frac{1}{2} n_2 n_1 2^{n_1/2}$

page 234, line -2: change $n_2 n_1 2^{n_1/2}$ to $\frac{1}{2} n_2 n_1 2^{n_1/2}$

page 239, line 9: change "x_1, she is still" to "x_0, she is still"

page 246, line -5: remove period after $p - 2$

page 247, line 2: add "(with $0 < r < p$)" at the end of the line

page 249, first lines of section 9.3: change "is at least as long as" to "can be longer than"

page 251, line 12: change "Exercise 9" to "Exercise 7"

page 252, line -5: add "Assume $\gcd(r, p - 1)$ is small."

page 253, line -8: remove "the"

page 278, lines -4, -3: change "Alice" to "Bob" and change "Bob" to "Alice"

page 282, line 7: change "form" to "from"

page 289, line 3: change "Exercise 9" to "Exercise 7"

page 289, lines 16, 17: change these lines to

$$h \equiv g^x \pmod{p}.$$

The number h is made public and identifies the bank.

page 298, line -6: change "s_t" to "s_{t-1}"

page 299, line -11: change "for $1 \le k \le t$" to "for $1 \le j \le t$"

page 318, step 1: **Comment:** We may assume $\gcd(r_1, n) = 1$ (otherwise, this gcd gives a factor of n)

page 319, line -14: change "$xv_1v_2v_4$" to "$xv_1^{-1}v_2^{-1}v_4^{-1}$"

page 319, line -13: change "$xv_{i_1}v_{i_2}\cdots v_{i_j}$" to "$xv_{i_1}^{-1}v_{i_2}^{-1}\cdots v_{i_j}^{-1}$"

page 320, line 3: change "$xv_1v_2v_4$" to "$xv_1^{-1}v_2^{-1}v_4^{-1}$"

page 320, line 4: change "xv_1v_3" to "$xv_1^{-1}v_3^{-1}$"

page 352, line 2: it should be $P_1 = (x_1, y_1)$

page 356, line -9: the beginning of the line should read "b. Then choose c so that "

page 356, line -8: change "choosing a and b" to "choosing b and c"

page 356, line -7: change "$a = 4$" to "$b = 4$"

page 356, line -6: change "b" to "c" (twice)

page 364, line -13: change "a=3" to "b=3"

page 364, line -12: change "b=45" to "c=45"

page 365, line 4: change "a=1" to "b=1"

page 365, line 4: change "b=7206" to "c=7206"

page 370, line 16: change $(0, 1)$ to $(2, 3)$

page 371, line 1: change "mod n" to "mod a prime p"

page 371, line 15: remove "mod n"

page 373, line -11: change $(0, 1)$ to $(2, 3)$

page 374, line 1: change "os" to "of"

page 374, line -7: indent part (f) less and remove "]"

page 403: line -9: change "$B(c, t)$" to "$B(c, r)$"

page 412, line 17: change "(0,0,0,0,0)" to "(0,0,0,0)"

(last updated 1/25/2020)