OLD DOMINION UNIVERSITY
CS 463

Homework 3

Madelene McFarlane

9/11/2023

#01096496

CS 463 Madelene McFarlane

HW 3

[ ] : answer

① $s_0 = 7$, $a = 12$, $b = 17$, $m = 23$

$s_{i+1} = (a \cdot s_i + b) \bmod m$

$i = 0 \rightarrow s_1 = (12 \cdot 7 + 17) \bmod 23 = (101) \bmod 23 = [9]$

$i = 1 \rightarrow s_2 = (12 \cdot 9 + 17) \bmod 23 = (125) \bmod 23 = [10]$

$i = 2 \rightarrow s_3 = (12 \cdot 10 + 17) \bmod 23 = (137) \bmod 23 = [22]$

$i = 3 \rightarrow s_4 = (12 \cdot 22 + 17) \bmod 23 = (281) \bmod 23 = [5]$

$i = 4 \rightarrow s_5 = (12 \cdot 5 + 17) \bmod 23 = (77) \bmod 23 = [8]$

$i = 5 \rightarrow s_6 = (12 \cdot 8 + 17) \bmod 23 = (113) \bmod 23 = [21]$

$i = 6 \rightarrow s_7 = (12 \cdot 21 + 17) \bmod 23 = (269) \bmod 23 = [16]$

$i = 7 \rightarrow s_8 = (12 \cdot 16 + 17) \bmod 23 = (205) \bmod 23 = [2]$

$i = 8 \rightarrow s_9 = (12 \cdot 2 + 17) \bmod 23 = (41) \bmod 23 = [18]$

$i = 9 \rightarrow s_{10} = (12 \cdot 18 + 17) \bmod 23 = (233) \bmod 23 = [3]$

CS 463 Madelene McFarlane

HW 3

bold = answer

(2) M = 5, FF = 00110

$S_0 = 00110$ $S_6 = 11001$ $S_{11} = 11010$ $S_{16} = 00011$ $S_{21} = 11001$

$S_1 = 00011$ $S_7 = 01100$ $S_{12} = 11101$ $S_{17} = 10001$ $S_{22} = 01100$

$S_2 = 10001$ $S_8 = 10110$ $S_{13} = 11110$ $S_{18} = 01000$ $S_{23} = 10110$

$S_3 = 01000$ $S_9 = 01011$ $S_{14} = 01111$ $S_{19} = 00100$ $S_{24} = 01011$

$S_4 = 00100$ $S_{10} = 10101$ $S_{15} = 00111$ $S_{20} = 10010$ $S_{25} = 10101$

$S_5 = 10010$

$S_{26} = 11010$ $S_{27} = 11101$ $S_{28} = 11110$ $S_{29} = 01111$ $S_{30} = 00111$

output = 01100010 01101011 **period Length = 15**

(3) R = 12ABCDEF K = 1A2B3C4D5E6F

→ 0001 0010 1010 1011 1100 1101 1110 1111 → 0001 1010 0010 1011 0011 1100 0100 1101 0101 1110 0110 1111

E(R) = 100010 100101 010101 010111 111001 011011 111101 011110

A = K1 ⊕ E(RD) = 100100 000111 111001 101011 101010 001110 000100 110001

B1 B2 B3 B4 B5 B6 B7 B8

B = S(A) = S(K ⊕ E(R)) → $S_1(B_1)\, S_2(B_2)\, S_3(B_3)\, S_4(B_4)\, S_5(B_5)\, S_6(B_6)\, S_7(B_7)\, S_8(B_8)$

$S_1(B_1) \rightarrow B_1 = 100100 \rightarrow 14 = \underline{1110}$

$S_2(B_2) \rightarrow B_2 = 000111 \rightarrow 7 = \underline{0111}$

$S_3(B_3) \rightarrow B_3 = 111001 \rightarrow 11 = \underline{1011}$

$S_4(B_4) \rightarrow B_4 = 101011 \rightarrow 1 = \underline{0001}$

$S_5(B_5) \rightarrow B_5 \rightarrow 101010 \rightarrow 13 = \underline{1101}$

$S_6(B_6) \rightarrow B_6 = 001110 \rightarrow 8 = \underline{1000}$

$S_7(B_7) \rightarrow B_7 = 000100 \rightarrow 2 = \underline{0010}$

$S_8(B_8) \rightarrow B_8 = 110001 \rightarrow 15 = \underline{1111}$

f(R, K) = P(B)

B = 1110 0111 1011 0001 1101 1000 0010 1111

P(B) = 1111 1101 1000 0110 1100 1111 0011 0100 = **FD86CF34**