Assignment 01

Instructor: Mehrdad Nojoumian
Course: Secret Sharing Protocols

Deadline: Feb 14

(1) Which one is a primitive root of 7?

a) 3 = {3, 2, 6, 4, 5, 1}

b) 5 = {5, 4, 6, 2, 3, 1}

c) 2 = {2, 4, 1}

(2) Find an inverse of "23" modulo "120". Also solve the following congruent equation $23x \equiv 3 \pmod{120}$ for x. Use the Euclid's Algorithm and the Extended Euclid's Algorithm.

47 (see Page 2), 21 = X

(3) Use the Fermat's little theorem to find: $3^{52} \pmod{11}$.

9

(4) What are the prime factorizations of "48" and "60"? Also, find GCD(48, 60) and LCM(48, 60).

$2^4 \times 3$, $3 \times 4 \times 5$, GCD(48, 60) = 12 LCM(48, 60) = 240

(5) What is the decimal expansion of $(1B6)_{16}$? What is the Hexadecimal expansion of "485"?

$(1B6)_{16} = 438_{10}$ $485_{10} = 1E5_{16}$

(6) What sequences of pseudorandom numbers is generated using the linear congruential generator $x_{n+1} = (4_{xn}+1) \bmod 7$ with seed $x_0 = 3$?

6 4 3 Repeats after 3

(7) The validity of an ISBN can be evaluated as explained in the class.

(Page 2)

- If the first 9 digits are "987654321", what is the check digit x_{10}? 0
- Is "9753842601" (where $x_1=9$ & $x_{10}=1$) a valid ISBN number? N 0

(8) Trace the Miller-Rabin probabilistic primality-test algorithm for a prime as well as a composite number. Provide details with respect to your tracing.

2) $23 \bmod 120$

$120 = 23*5 + 5$

$23 = 5*4 + 3$

$5 = 3*1 + 2$

$3 = 2*1 + 1$

$2 = 1*2 + 0$

Relatively Prime

$1 = 3 - 2*1$

$1 = 3 - [5 - 3*1]*1 = 3 - 5*1 + 3*1 = -1*5 + 2*3$

$= -1*5 + 2*[23 - 5*4] = -1*5 + 2*23 - 5*8$

$= -9*5 + 2*23$

$= -9*[120 - 23*5] + 2*23$

$= -9*120 + 45*23 + 2*23$

$= -9*120 + 47*23$

$47 = 23^{-1} \bmod 120$ $47*23 =$

$23x = 3 \bmod 120$

$47*23x = 47*3 \bmod 120$

$x = 141 \bmod 120$

$x = 21$

3) $3^{52} \bmod 11 = (3^{5*10})(3^2) \bmod 11$ $1 = 3^{10} \bmod 11$

$= 9$

4) $1B6_{16} = 256 + 11*16 + 6$

$= 256$

176

6

438_{10}

256 | 485 (1) — 256 — 229

16 | 229 (14) — 16 — 69 — 64 — 5

1 E 5_{16}

7) ISBN: 987654321

$(9*1 + 8*2 + 7*3 + 6*4 + 5*5 + 4*6 + 3*7 + 2*8 + 1*9) \bmod 11$

$(9 + 16 + 21 + 24 + 25 + 24 + 21 + 16 + 9) \bmod 11$

$[2(9 + 16 + 21 + 24) + 25] \bmod 11 = [2(70) + 25] \bmod 11 = 165 \bmod 11 = 0$

ISBN: 975384261

$[(9*1 + 7*2 + 5*3 + 3*4 + 8*5 + 4*6 + 2*7 + 6*8 + 10*9)] \bmod 11 \stackrel{?}{=} 1$

$[9 + 14 + 15 + 12 + 40 + 24 + 14 + 48] \bmod 11 \stackrel{?}{=}$

$176 \bmod 11 \stackrel{?}{=}$

$0 \stackrel{?}{=} 1$ NO

Miller-Rabin

a) Test: 113

$t = 3$

$112 = 2^4 * 7$

For $i = 1$ to 3

$a = 2$

$y = 2^7 \bmod 113 = 15$

$15 \neq 1$ and $15 \neq 112$

$j = 1$

While $1 < 3$ and $15 \neq 112$ ($y \neq N-1$)

$y \leftarrow y^2 \bmod 113 = 12$

$j \leftarrow 2$

$y \leftarrow y^2 \bmod 113 = 31$

$j = 3$

$i = 2$

$a = 13$

$y = 13^7 \bmod 113 = 69$

$69 \neq 1$ and $69 \neq 112$

$j = 1$

While $j(1) < 3$ & $69 \neq 112$ (y)

$y \leftarrow y^2 \bmod 113 = 15$

$j \leftarrow 2$

$y \leftarrow y^2 \bmod 113 = 112$

IF $y = 1$ return composite

IF $y \neq N-1$ composite

Return PRIME

Test: $57 = 3 * 17$

$n = 57, s = 3$

For $j = 1$ to 3 $s = 1$

$a \leftarrow 7$

$56 = 2^3 * 7$

$y = 7^7 \bmod 57 = 7$

If $y \neq 1$ and $y \neq 56$ ✓

$i = 1$

while $i \leq 2$ & $y \neq 56$

$y \leftarrow y^2 \bmod 57 = 49$

$i = 2$

$y \leftarrow 49^2 \bmod 57 = 7$

$i = 3$

$j = 2$

$a = 11$

$56 = 2^3 * 7$

$y = 11^7 \bmod 57 = 11$

If $y \neq 1$ & $y \neq 56$ ✓

$i = 1$

while $i \leq 2$ & $y \neq 56$

$y = y^2 \bmod 57 = 7$

$i = 2$

$y = 7^2 \bmod 57 = 49$

$i = 3$

$j = 3$

$a = 13$

$56 = 2^3 * 7$

$y = 13^7 \bmod 57 = 10$

If $y \neq 1$ & $y \neq 56$ ✓

$i = 1$ while

while $i \leq 2$ & $y \neq 56$

$y = y^2 \bmod 57 = 10^2 \bmod 57 = 43$

$i = 2$

$y = y^2 \bmod 57 = 43^2 \bmod 57 = 25$

$y \neq 56$ return composite