Christopher Foley
Z15092976

Assignment 01

Instructor: Mehrdad Nojoumian
Course: Practical Aspects of Modern Cryptography

Deadline: September 29

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

a) 3

b) 5

c) 2

(2) Find an inverse of "23" modulo "120". Also solve $23x \equiv 3 \pmod{120}$ for "x".
(Hint: Use Euclid's Algorithm & Extended Euclid's Algorithm)

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

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

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

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

(7) Encrypt the message STOP POLLUTION by translating the letters into numbers, applying the given encryption function, and then translating the numbers back into letters:

$$f(x) = (17x + 22) \bmod 26$$

(8) Decrypt the following message that were encrypted using the Caesar shift:

EOXH MHDQV

(9) Encrypt the message GRIZZLY BEARS using blocks of five letters and the transposition cipher based on the permutation of {1, 2, 3, 4, 5} with $\sigma(1) = 3$, $\sigma(2) = 5$, $\sigma(3) = 1$, $\sigma(4) = 2$ and $\sigma(5) = 4$. For this exercise, use the letter X as many times as necessary to fill out the final block of fewer than five letters.

Christopher Foley
215092976

Assignment 1 2/5

① Primitive Root of 7

a) $3^1=3, 3^2=2, 3^3=6, 3^4=4, 3^5=5, 3^6=1$ $\{3,2,6,4,5,1\}$ yes

b) $5^1=5, 5^2=4, 5^3=6, 5^4=2, 5^5=3, 5^6=1$ $\{5,4,6,2,3,1\}$ yes

c) $2^1=2, 2^2=4, 2^3=1$. $\{2,4,1\}$ NO

② $23 \bmod 120$ Solve $23x \equiv 1 \bmod 120$

Check to see if 23, 120 relatively prime

$120 = 23\times5 + 5$

$23 = 5\times4 + 3$

$5 = 3\times1 + 2$

$3 = 2\times1 + 1$

$2 = 1\times2 + 0$

Now

$1 = 3 - 2 = 3-(5-3\times1) = 3+5+3\times1 = -5+3\times2$

$= -5+3\times2 = -5+2(23-5\times4) = -5+2\times23-5\times8$

$= 2\times23-9\times5 = 2\times23-9(120-23\times5) = 2\times23-9\times120+23\times45$

$= 47\times23-9\times120$

$\therefore 1 \equiv 47\times23 \bmod 120$

$23x \equiv 3 \bmod 120$

$47\times23x \equiv 47\times3 \bmod 120$

$x \equiv 141 \bmod 120$

$x \equiv 21 \bmod 120$

③ $3^{52} \bmod 11$

We know $3^{10} \equiv 1 \bmod 11$ therefore

$3^{52} = (3^{10})^5 3^2$

$3^2 \bmod 11 = 9$

④ $48 = 2^4\cdot3 = 2\cdot2\cdot2\cdot2\cdot3$

$60 = 2^2\cdot3\cdot5 = 2\cdot2\cdot3\cdot5$

Foley 3/5

2 | 48 60
2 | 24 30
3 | 12 15
4 5

$gcd(48,60) = 2^2 \times 3 = 12$
$lcm(48,60) = 2^2 \times 3 \times 4.5 = 240$

5) $1B6_{16} = 256 + 11 \times 16 + 6 = 256 + 176 + 6 = 438$

2 | 485 | 1
2 | 242 | 0
1 | 21 | 1
6 | 0 | 0
3 | 0 | 0
1 | 5 | 1
7 | 1
3 | 1
1 | 1
0

$485_{10} = 1E9_{16}$

6) $X_{n+1} = (4x_n + 1) \bmod 7 \quad x_0 = 3$
$\{3, 6, 4\}$

7) Encode "STOP POLLUTION" Let A=00 B=01
To Numbers: 18 19 14 15 15 14 11 11 20 19 08 14 13
$f(x) = (17x + 22) \bmod 26 = 17x \bmod 26 + 22 \bmod 26$
$= 16\ 07\ 00\ 17\ 17\ 00\ 01\ 01\ 24\ 07\ 02\ 00\ 09$
To Letters: "QHARRABBYHCAJ"
See Appendix A for inverse
Inverse Function: $f^{-1}(x) = (23x - 12) \bmod 26$
18 19 14 15 15 14 11 11 20 19 08 14 13
Checks

Foley 4/5

8) Caesar Shift: EOXH MHDQV

Looking At Letters we need to determine the shift

45 4F 58 48 —

Guess of X+3 to encode X-3 to decode

Since that was used in class we got

BLUE JEANS

otherwise we would try different values of

(X-n) mod 26 to get plaintext

9) GRIZZLYBEARSXXX

σ(1)=3 σ(2)=5 σ(3)=1 σ(4)=2 σ(5)=4

becomes

IZGZRBELAYXXRXS

Appendix A

Find inverse of $f(x) = 17x + 22 \mod 26$

$y = 17x + 22$

$x = 17y + 22$

$17y = x - 22$

$y = \overline{17}(x - 22)$

Find inverse of $17 \mod 26$

$26 = 17 \times 1 + 9$

$17 = 9 \times 1 + 8$

$9 = 8 \times 1 + 1$

$8 = 8 \times 1 + 0$

$1 = 9 - 8 = 9 - (17 - 9 \times 1) = 9 \times 2 - 17$

$= -17 + 9 \times 2 = -17 + 2(26 - 17 \times 1)$

$= -17 + 26 \times 2 - 17 \times 2 = 26 \times 2 - 17 \times 3$

$= -3 \times 17 = 23 \times 17$

Therefore

$f^{-1}(x) = 23(x - 22) \mod 26$

$= (23x - 12) \mod 26$