Rifa
Safeer
Shah

Homework 3: Cryptography 09/24/2019

1. Encrypt the message DO NOT PASS GO by translating the letters into numbers, applying the given encryption function, and then translating the numbers back into letters.

a) $f(p) = (p+3) \bmod 26$

DO NOT PASS GO

3 14 13 14 19 15 0 18 18 6 14

6 17 16 17 22 18 3 21 21 9 17

GR QRW SDVV JR

b) $f(p) = (p+7) \bmod 26$

DO NOT PASS GO

3 14 13 14 19 15 0 18 18 6 14

10 21 20 21 0 22 7 25 25 13 21

KV UVA WHZZ NV

c) $f(p) = (5p+2) \bmod 26$

DO NOT PASS GO

3 14 13 14 19 15 0 18 18 6 14

17 20 15 20 19 25 2 14 14 6 20

RU PUT ZCOO GU

2. Decrypt these messages that were encrypted using $f(p) = (p+3) \bmod 26$

a) EOXH MHDQV

4 14 23 7 12 7 3 16 21

1 11 20 4 9 4 0 13 18

BLUE JEANS

b) WHVW WRGDB

22 7 21 22 22 17 6 3 1

19 4 18 19 19 14 3 0 24

TEST TODAY

Rifa
Safeer
Shah

Homework 3: Cryptography 09/24/2019

c) HDW GLP VXP

7 3 22 6 11 15 21 23 15

4 0 19 3 8 12 18 20 12

EAT DIM SUM

3 Alice wants to send to all her friends, including Bob, the message "GET OUT NOW" so that he knows that she sent it. What should she send to her friends, assuming she signs the message using the RSA cryptosystem.

GET OUT NOW

6419 142019 131422

Key (2537, 13)

$2537 = 43 \cdot 59$

$p = 43$, $q = 59$

$\gcd(13, (43-1)(59-1)) = 1 \rightarrow 13(42 \cdot 58) = 1$

06 04 19 14 20 19 13 14 22 00

$C = M^{13} \bmod 2537$

$0604^{13} \bmod 2537 = 495$

$1914^{13} \bmod 2537 = 2367$

$2019^{13} \bmod 2537 = 150$

$1314^{13} \bmod 2537 = 2431$

$2200^{13} \bmod 2537 = 1254$

Encrypted message: 0495 2367 0150 2431 1254

4. Find the following using Fermat's Little Theorem

a) $6^{212} \bmod 11$

$a^{p-1} = 1 \pmod p$

$6^{10} = 1 \pmod{11}$

$6^{212} = 6^{(10 * 21 + 2)}$

$6^2 \cdot (6^{10})^{21} = 6^2 \bmod 11$

$6^{212} = 36 \bmod 11$

$6^{212} = 3$

Rifa
Safeer
Shah

09/24/2019

Homework 3: Cryptography

b) $8^{145} \bmod 13$

$a^{p-1} \equiv 1 \pmod{p}$

$8^{13-1} \equiv 1 \pmod{13}$

$8^{145} \equiv (8^{12})^{12} \cdot 8^1$

$8 * 8^{144} \equiv 8 \times 1 \pmod{13}$

$8^{145} \equiv 8 \bmod 13$

$8 \bmod 13 \equiv 8$