Gloire Rubambiza
02/28/2018
MTH 312

# Assessment 2 – Question 4

4.a) $35^{10} \bmod 127$

$35^1 \bmod 127 = 35$

$35^2 \bmod 127 = (35 \bmod 127 \cdot 35 \bmod 127) \bmod 127$

$= 35^2 \bmod 127$

$= 82$ *

$35^4 \bmod 127 = (35^2 \bmod 127 \cdot 35^2 \bmod 127) \bmod 127$

$= 82^2 \bmod 127$

$= 120$

$35^8 \bmod 127 = (35^4 \bmod 127 \cdot 35^4 \bmod 127) \bmod 127$

$= 120^2 \bmod 127$

$= 49$ *

$35^{10} \bmod 127 = (35^8 \bmod 127 \cdot 35^2 \bmod 127) \bmod 127$

$= (49 \cdot 82) \bmod 127$

$= \boxed{81}$ ✓

4.b) $23^{12} \bmod 50$

$23^2 \bmod 50 = (23 \bmod 50 \cdot 23 \bmod 50) \bmod 50$

$= 23^2 \bmod 50$

$= 29$

$23^4 \bmod 50 = (23^2 \bmod 50 \cdot 23^2 \bmod 50) \bmod 50$

$= 29^2 \bmod 50$

$= 41$ *

$23^8 \bmod 50 = (23^4 \bmod 50 \cdot 23^4 \bmod 50) \bmod 50$

$= 41^2 \bmod 50$

$= 31$ *

$23^{12} \bmod 50 = (23^8 \bmod 50 \cdot 23^4 \bmod 50) \bmod 50$

$= 41 \cdot 31 \bmod 50$

$= \boxed{21}$ ✓

Gloire Rubambiza
MTH 312
02/28/2018

# Assessment 2 - Question 5

5.a) Clear text : SPRING

Matching text = AGDGXAXDAAGG

| B | R | E | A | K |
|---|---|---|---|---|
| A | G | D | G | X |
| A | X | D | A | A |
| G | G | | | |

| A | B | E | K | R |
|---|---|---|---|---|
| G | A | D | X | G |
| A | A | D | A | X |
| | G | | | G |

Encryption : GAAAGDGXAGXG
GAAAVDDXAGXG

5. b)

| A | C | D | R |
|---|---|---|---|
| G | D | A | D |
| A | G | D | F |
| D | X | A | A |
| G | V | | |

| C | A | R | D |
|---|---|---|---|
| D | G | D | A |
| G | A | F | D |
| X | D | A | A |
| V | G | | |

Decrypted : PLAYING

Gloire Rubambiza
02/28/2018
MTH 312

## Assessment 2 - Question 7

7.a) C o l d $\sqcup$ A i r
28 14 11 3 62 26 8 17

$x \to (15x + 13) \bmod 67$

$C \to 28 \to (15 \cdot 28 + 13) \bmod 67 = 31 = F$

$o \to 14 \to (15 \cdot 14 + 13) \bmod 67 = 22 = w$

$l \to 11 \to (15 \cdot 11 + 13) \bmod 67 = 44 = S$

$d \to 3 \to (15 \cdot 3 + 13) \bmod 67 = 58 = 6$

$\sqcup \to 62 \to (15 \cdot 62 + 13) \bmod 67 = 5 = f$

$A \to 26 \to (15 \cdot 26 + 13) \bmod 67 = 1 = b$

$i \to 8 \to (15 \cdot 8 + 13) \bmod 67 = 66 = ?$

$r \to 17 \to (15 \cdot 17 + 13) \bmod 67 = 0 = a$

Cipher text = FwS6fb?a ✓

b) g z C .
6 25 28 63

$f(x) = (7x + 4) \bmod 67$

gcf $(7, 67) = 1 \to$ multiplicative inverse exists

$1 = m \cdot 7 + k \cdot 67$

$67 = 9 \cdot 7 + 4$

$$\begin{bmatrix} 67 \\ 1 \\ 0 \end{bmatrix} - 9 \begin{bmatrix} 7 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 4 \\ 1 \\ -9 \end{bmatrix}$$

$$\begin{bmatrix} 7 \\ 0 \\ 1 \end{bmatrix} - 1 \begin{bmatrix} 4 \\ 1 \\ -9 \end{bmatrix} = \begin{bmatrix} 3 \\ -1 \\ 10 \end{bmatrix}$$

$$\begin{bmatrix} 4 \\ 1 \\ -9 \end{bmatrix} - 1 \begin{bmatrix} 3 \\ -1 \\ 10 \end{bmatrix} = \begin{bmatrix} 1 \\ 2 \\ -19 \end{bmatrix}$$

$$\begin{bmatrix} 3 \\ -1 \\ 10 \end{bmatrix} - 3 \begin{bmatrix} 1 \\ 2 \\ -19 \end{bmatrix} = \begin{bmatrix} 0 \\ -7 \\ 67 \end{bmatrix}$$

$\Rightarrow 1 = 2 \cdot 67 + -19 \cdot 7$

Gloire Kubambiza
02/22/2018
MTH 312

## Assessment 2 - Question 7 (Continued)

7.b continued

Translation

$g \rightarrow 6 = (7x+4) \bmod 67$

"subtract 4" $2 \bmod 67 = 7x \bmod 67$

"unmultiply" by 7 $-19 \cdot 2 \bmod 67 = -19 \cdot 7x \bmod 67$

$-38 \bmod 67 = x$

$x = 29 = D$

$Z \rightarrow 25 = 21 \bmod 67 = 7x \bmod 67$

$-19 \cdot 21 \bmod 67 = -19 \cdot 7x \bmod 67$

$-399 \bmod 67 = x$

$x = 3 = d$

$E \rightarrow 28 = 24 \bmod 67 = 7x \bmod 67$

$-19 \cdot 24 \bmod 67 = -19 \cdot 7x \bmod 67$

$-456 \bmod 67 = x$

$x = 13 = n$

$o \rightarrow 63 = 59 \bmod 67 = 7x \bmod 67$

$-19 \cdot 59 \bmod 67 = -19 \cdot 7x \bmod 67$

$-1121 \bmod 67 = x$

$x = 18 = s$

Decrypted text = Ddns ✓

Gloire Rubambiza
02/28/2018
MTH 312

Assessment - Question 9

9.a) 0101 | 1000 | 0101 | 1001
K 1010 1000 1010 1000
Cipher = 1111 | 0000 | 1111 | 0001 ✓

b) 1110 | 0111 | 1110 | 0011
1010 1000 1010 1000
Cipher = 0110 1111 0101 1011
~~0100 1111 0100 1011~~

1 if the digits are different

0 if the digits are the same