Cryptography – Multiplying Matrices (Ch 10.4) v--. Name(s)

Algebra 2 Date Period

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **A** | **B** | **C** | **D** | **E** | **F** | **G** | **H** | **I** | **J** | **K** | **L** | **M** | **N** | **O** | **P** | **Q** | **R** | **S** | **T** | **U** | **V** | **W** | **X** | **Y** | **Z** |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Space** | **!** | **@** | **#** | **$** | **%** | **^** | **&** | **\*** | **(** | **)** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **0** | **+** | **-** | **.** | **?** |
| 0 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 | 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 | 49 | 50 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Let **A** = Matrix Key - dimension: 2**×**2 - random numbers **B** = Message (Original) - dimension: 2**×**n **C** = Message (Coded) | **A ×** **B****A-1** **×** **A** **×** **B****B**  | === | C**A-1** **×** **C****A-1** **×** **C** | Encode the Original w/ KeyTo decode, multiply by the Inverse (of the Key) |

EX) Message: M E E T M E @ 7 P M .

Unencoded Message: 13**|**5**|**5**|**20**|**0**|**13**|**5**|**0**|**28**|**43**|**16**|**13**|**49

**A ×** **B** =  =  = **C**

Encoded Message: 13**|**61**|**91**|**52**|**26**|**111**|**5**|**39**|**127**|**187**|**124**|**52**|**235**|**15

To decode, find **A-1**.

**B** = **A-1** **×** **C** = =

Match numbers to characters: 13 = M, 5 = E, 5 = E, 20 = T, 0 = Space, etc…

Encode the following messages. Use **A** = .

1) ABORT MISSION. Unencoded Message:

**A ×** **B** = = 

 Encoded Message:

2) RENDEZVOUS @ K-MART! Unencoded Message:

**A ×** **B** = = 

Encoded Message:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **A** | **B** | **C** | **D** | **E** | **F** | **G** | **H** | **I** | **J** | **K** | **L** | **M** | **N** | **O** | **P** | **Q** | **R** | **S** | **T** | **U** | **V** | **W** | **X** | **Y** | **Z** |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Space** | **!** | **@** | **#** | **$** | **%** | **^** | **&** | **\*** | **(** | **)** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **0** | **+** | **-** | **.** | **?** |
| 0 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 | 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 | 49 | 50 |

Decode the following messages. Use **A** = .

3) -32**|**-30**|**-6**|**-42**|**-38**|**0**|**88**|**90**|**18**|**126**|**114**|**0

**A-1** =  ⇨ **B** = **A-1** **×** **C** =  ⇨

 =  Decoded Message:

4) -2**|**-38**|**0**|**-24**|**-2**|**-28**|**-8**|**-10**|**-8**|**-98**|**0**|**25**|**103**|**5**|**60**|**10**|**71**|**27**|**37**|**25**|**245**|**8

**A-1** =  ⇨ **B** = **A-1** **×** **C** =  ⇨

 =  Decoded Message:

5) -16**|**-10**|**0**|**-12**|**-24**|**-18**|**-32**|**-38**|**-18**|**-8**|**-10**|**-98**|**59**|**30**|**5**|**30**|**85**|**60**|**101**|**95**|**60**|**34**|**25**|**265

**A-1** =  ⇨ **B** = **A-1** **×** **C** =  ⇨

 =  Decoded Message: