

# Primer Examen Parcial - Introducción a la Criptografía y a la Seguridad de la Información

7 de Octubre de 2020

1. Usted interceptó el mensaje cifrado  $c = 4, 13, 18, 20, 15, 12$  que fue cifrado con HILL en  $\mathbb{Z}_{29}$  con bloques de tamaño  $t = 3$ . Si la matriz de cifrado era  $K = \begin{pmatrix} 12 & 3 & 4 \\ 24 & 28 & 12 \\ 24 & 20 & 24 \end{pmatrix}$ , diga cual es el mensaje limpio.
2. Usted interceptó el siguiente mensaje cifrado con Playfair (en esta version de Playfair siempre que toque completar caracteres se completan con la letra X):

QUAYGDKFTSDLFRNDDBKELBUKGSVAPUBRQFGQ

Descifre el mensaje.

Ayuda: El mensaje esta en español sin espacios.

3. Considere el alfabeto  $\Sigma = \{A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y, Z, \text{espacio}\}$  y los sistemas de cifrado  $E_{k_1}^{(1)} = \text{Cesar}$  y  $E_{k_2}^{(2)} = \text{HomofonicoExamen}$ . HomofonicoExamen es un sistema de cifrado similar al Homofonico que considera elementos sobre el alfabeto  $\Sigma$  tanto en los mensajes como en la llave, pero donde los elementos se cifran bajo una distribución uniforme, es decir, a cada elemento del alfabeto en el texto limpio le corresponden 5 elementos en el texto cifrado, dando 135 elementos (identificados desde 0 hasta 134).  
Usted interceptó el siguiente mensaje cifrado con  $E_{k_2}^{(2)} \circ E_{k_1}^{(1)}$ :

98 94 44 29 16 37 27 110 100 68 31 79 2 9 130 36 13 29 88 40 68 127 2 0 58 39 6 83 68 94 100 85 56 30 68 112 113 114  
81 88 112 85 2 33 57 91 68 122 86 31 0 128 2 9 130 13 105 68 67 76 0 40 79 116 112 82 18 47 25 115 2 73 68 92 35 62 0  
127 108 76 68 31 3 2 110 134 47 64 87 41 0 20 33 68 70 31 47 92 13 134 110 35 8 116 42 82 9 13 4 40 85 18 24 13 41 68  
24 42 0 73 39 32 85 33 87 107 108 116 3 116 68 33 42 114 120 85 128 108 42 9 41 108 50 89 77 9 12 27 2 2 16 9 8 92 79  
0 131 2 0 105 35 126 68 31 92 44 4 25 9 41 67 37 103 27 134 68 58 88 57 44 88 38 116 85 92 50 104 68 35 3 47 133 32 9  
80 31 112 0 113 87 41 85 37 28 13 36 128 45 103 47 13 9 112 116 59 16 88 128 47 8 88 47 15 49 128 88 68 24 80 119 47  
77 56 119 75 110 116 40 2 29 76 57 27 85 128 15 106 115 25 68 62 42 68 51 13 54 76 68 106 128 47 11 74 68 18 86 47  
96 37 127 0 67 106 119 0 32 49 59 61 116 77 68 7 44 45 23 67 9 107 79 126 110 40 113 18 0 24 37 45 101 85 56 84 85 44  
7 85 67 20 130 0 57 80 12 76 47 40 88 81 76 4 77 88 40 68 87 113 68 50 128 68 92 116 100 9 127 86 87 85 17 16 44 76  
115 22 134 1 47 62 80 31 108 68 130 33 70 74 76 85 49 4 77 0 31 92 42 0 51 35 3 37 9 100 41 126 22 88 4 18 32 47 72  
88 41 85 31 108 120 79 62 33 85 79 56 127 68 18 67 88 68 58 37 18 41 88 29 68 67 42 45 27 9 18 24 20 115 83 85 70 4  
40 9 77 86 113 128 0 17 86 89 96 88 18 0 107 42 16 42 85 82 86 128 85 130 11 66 30 86 32 88 40 68 127 35 68 61 115 2  
8 9 114 58 2 94 31 68 128 24 116 68 130 128 2 4 42 9 87 29 0 7 45 133 7 7 91 0 31 108 70 41 45 134 47 127 13 19 76 47  
49 68 57 35 31 85 87 52 9 88 28 74 45 49 80 4 50 115 96 68 108 37 89 117 20 2 4 37 68 27 2 79 83 76 40 9 36 35 33 43  
44 4 118 37 40 47 5 11 41 47 3 86 115 68 54 44 131 82 41 47 20 52 47 107 88 0 55 126 84 128 47 77 2 85 49 47 58 20 18  
68 79 12 9 101 87 19 20 33 96 85 13 29 86 94 82 40 47 82 86 0 32 13 50 22 85 15 49 120 120 1 47 7 110 114 41 110 1 68  
102 88 63 76 47 40 79 82 88 85 116 82 2 133 96 67 68 30 86 83 106 82 72 85 114 29 35 11 115 54 47 92 42 0 101 11 27  
134 76 54 0 70 47 119 70 74 85 87 7 85 21 56 74 50 41 37 120 68 31 79 73 70 120 22 68 15 44 119 85 13 4 22 85 130 128  
114 16 41 42 22 0 41 79 47 110 88 39 89 82 85 18 24 37 0 82 49 95 116 100 68 87 12 9 50 128 100 9 95 87 86 113 112 85  
18 15 76 0 52 87 57 45 79 107 20 33 72 47 51 86 89 4 50 82 72 68 115 87 128 37 32 47 8 37 29 76 47 131 42 134 80 14  
76 89 116 131 9 31 86 9 67 13 29 120 103 47 24 37 120 95 106 35 4 42 0 13 33 54 85 33 88 43 80 57 110 37 85 70 128 47  
127 92 76 68 5 3 42 39 61 12 114 112 127 9 31 39 121 45 37 68 128 15 42 91 0 73 76 16 116 85 13 134 45 9 127 15 42 9  
84 49 95 76 68 105 86 126 89 68 131 42 18 88 82 18 80 79 115 85 102 50 27 57 85 41 13 61 42 47 30 110 49 118 76 9 39  
41 85 116 110 116 43 76 4 85 87 6 134 79 118 61 0 18 35 115 20 96 24 127 47 117 116 37 128 9 104 89 85 17 44 134 36  
15 85 50 115 85 18 24 88 85 88 82 127 16 114 82 118 37 85 24 114 27 57 9 74 16 87 69 116 130 112 35 3 68 119 6 122  
86 33 70 72 70 110 134 9 24 13 89 3 105 9 24 70 77 85 69 2 120 122 2 18 18 88 33 85 128 67 76 91 9 32 18 50 134 110 0

67 39 40 85 131 88 127 88 82 41 20 35 33 100 85 128 86 0 22 35 85 44 4 68 128 108 88 68 17 133 29 35 16 9 35 14 88 29  
85 41 67 116 85 30 35 80 115 128 112 47 18 15 88 103 40 68 27 79 100 18 47 92 76 85 15 114 57 7 68 116 124 101 42 6  
31 42 77 9 108 76 29 95 20 35 4 37 0 18 86 0 6 35 104 74 57 13 50 4 68 41 108 70 128 85 18 15 50 130 68 73 114 32 85  
114 47 107 67 35 27 88 0 4 80 72 108 127 9 2 69 47 100 18 56 131 103 20 113 96 0 57 35 130 127 9 78 56 31 85 112 15  
88 47 131 20 40 82 127 47 32 49 91 0 49 0 73 2 120 54 85 27 44 19 42 9 108 13 16 3 91 0 130 24 88 68 12 88 110 41 85  
127 15 42 105 47 131 42 112 37 89 63 76 54 0 8 92 39 127 0 31 108 88 1 131 85 64 2 128 47 13 18 9 37 27 88 14 88 82 9  
86 23 45 79 36 93 85 128 108 13 18 9 82 20 64 24 18 68 18 92 88 105 68 130 39 20 40 9 64 79 87 131 75 65 116 0 41 86  
68 16 86 113 9 50 115 68 41 24 116 68 36 86 117 119 35 4 0 120 2 87 95 68 13 82 54 9 8 42 113 18 85 40 86 8 113 9 18  
35 47 18 24 88 9 37 115 127 3 70 82 118 42 0 15 114 57 110 85 102 80 128 92 47 82 88 14 50 27 27 37 9 69 20 110 36  
108 0 8 39 112 68 49 27 29 88 13 22 103 47 128 67 88 120 76 68 114 115 40 0 130 79 47 107 114 32 85 119 13 45 17 79  
1 47 67 13 3 16 1 0 24 114 77 85 114 45 100 35 0 7 79 16 99 87 128 31 42 82 68 18 92 49 41 9 117 49 27 12 87 103 0 24  
49 22 68 122 35 128 18 42 4 47 39 68 131 37 127 76 82 31 106 35 33 9 127 2 86 85 12 87 27 57 35 62 9 117 116 9 32 114  
106 77 47 52 80 110 118 92 68 134 80 64 92 128 106 4 64 0 114 9 110 13 119 101 0 114 33 54 47 134 37 13 40 44 113 72  
0 127 108 37 104 47 79 56 128 32 50 54 42 0 80 85 58 37 41 85 103 2 94 134 27 85 41 92 80 82 19 9 127 102 50 118 116  
9 70 121 86 56 128 9 78 3 76 39 61 80 4 122 68 13 47 100 59 67 86 79 110 9 3 11 45 88 68 49 122 39 80 82 9 102 35 82  
31 68 65 35 11 68 116 108 68 92 37 68 32 114 20 40 0 27 37 37 89 50 113 99 85 70 128 68 127 24 37 51 0 79 24 0 1 76  
32 85 15 13 120 54 68 73 79 120 25 85 114 82 77 85 101 13 106 4 68 39 3 42 47 127 15 88 9 121 88 130 31 68 18 37 70 6  
92 116 29 32 9 50 17 0 65 87 133 9 39 84 19 47 117 116 47 50 18 84 85 71 133 84 128 0 70 85 101 44 31 65 9 31 24 116  
105 47 57 76 127 68 31 108 116 68 86 57 77 9 30 133 4 80 32 67 117 76 115 128 32 9 131 50 76 47 35 94 127 47 108 49  
113 99 47 103 86 11 85 121 105 0 103 79 11 16 0 8 29 106 130 18 112 0 12 16 79 119 85 18 67 76 9 36 116 50 45 50 113  
122 85 17 35 29 9 70 85 7 88 102 68 131 114 103 112 9 20 43 37 68 64 86 41 9 128 15 76 9 6 67 13 106 115 32 47 84 127  
20 134 134 68 106 4 68 104 105 9 2 7 12 50 6 88 68 19 116 37 66 9 88 95 0 62 37 27 110 85 87 106 110 37 54 68 50 115  
0 23 39 84 37 68 18 15 76 65 120 37 9 42 14 42 89 9 115 116 88 131 37 131 47 3 106 96 108 128 85 87 17 17 0 62 76 85  
72 86 47 49 4 22 85 22 86 82 31 68 127 67 50 33 61 68 87 7 9 29 56 115 33 80 33 99 47 87 7 7 85 113 87 107 68 20 128  
57 57 9 75 42 68 8 79 16 130 76 68 69 2 29 0 1 79 56 9 80 69 47 105 86 126 68 131 35 68 31 92 42 105 85 104 39 16 118  
24 116 54 47 86 69 12 68 13 36 3 35 112 84 68 127 92 88 85 22 70 16 25 68 99 89 2 94 113 77 100 47 4 37 43 106 134 45  
37 47 61 37 101 128 9 32 115 44 7 17 50 4 64 85 92 39 16 89 91 68 8 79 82 40 76 29 76 40 85 102 24 70 31 0 18 15 37  
50 89 9 81 133 33 20 84 108 104 37 113 18 0 107 70 32 85 96 2 106 82 96 9 31 86 68 78 88 9 50 127 9 117 94 84 41 85  
78 88 85 84 79 119 116 128 15 44 115 122 0 120 42 114 57 110 91 47 24 2 29 120 80 58 110 116 0 86 89 47 69 50 45 118  
67 68 73 2 56 27 54 115 127 9 58 116 0 84 35 56 4 77 50 82 96 85 100 2 85 131 116 134 20 99 108 31 116 54 9 31 108 88  
9 51 79 2 4 9 107 13 112 0 75 3 106 122 108 31 68 121 133 31 47 36 45 79 56 77 130 85 32 6 56 54 77 20 82 64 0 114 36  
89 35 100 130 68 20 127 9 61 88 74 18 9 127 92 16 79 62 50 4 96 0 18 24 42 95 9 44 82 18 87 9 40 70 29 61 4 37 112 84  
68 13 24 116 39 22 47 24 49 3 3 103 68 36 79 126 27 54 85 32 37 42 9 18 15 42 47 134 80 122 24 18 42 131 0 8 50 33 40  
87 107 112 0 87 12 68 108 114 96 89 20 54 130 9 24 94 128 0 128 92 88 4 68 18 67 42 103 9 24 37 70 3 77 68 70 0 22 20  
84 31 49 4 41 9 112 108 87 56 41 9 80 84 0 18 15 114 127 47 105 86 11 9 52 50 45 36 15 85 24 126 16 16 65 9 11 101 68  
106 0 73 13 113 31 68 18 76 120 0 122 37 18 85 84 41 39 16 31 42 77 9

Descifre el mensaje.

Nota: El cifrado Cesar deja los espacios tal cual.

Ayuda: El texto esta en ingles y tiene que ver con Harry Potter.