*****Instituto Politécnico Nacional***

***Escuela Superior de Cómputo***

*Criptography*

***Ejercicios Capítulo I***

***Nombre:*** *Sampayo Hernández Mauro*

***Grupo:*** *3CV17*

***Profesor:*** *Víctor Manuel Silva García*

**Ejercicios.**

1. **Construya un Sistema de cifrado Vigenere, utilizando como clave su nombre y como texto plano Escuela Superior de Cómputo, además, conteste las siguientes preguntas:**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A | B | C | D | E | F | G | H | I | J | K | L | M | N |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
| Ñ | O | P | Q | R | S | T | U | V | W | X | Y | Z |  |
| 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Mensaje | E | S | C | U | E | L | A | S | U | P | E | R | I | O | R | D | E | C | O | M | P | U | T | O |
| Clave | M | A | U | R | O | M | A | U | R | O | M | A | U | R | O | M | A | U | R | O | M | A | U | R |
| Mensaje cifrado | P | S | W | M | S | W | A | N | M | E | P | R | C | G | G | O | E | W | G | A | B | U | Ñ | G |

1. **Diga cuál es el conjunto de textos planos .**
2. **Diga cuál es el conjunto de textos cifrados .**
3. **Diga cuál es el conjunto de llaves .**

La clave “Mauro” tiene 5 letras, por lo tanto:

1. **Proponga un texto plano, y posteriormente aplique una permutación sobre las posiciones para obtener el texto cifrado. Por otro lado, resuelva el siguiente inciso.**

Se propone el texto siguiente: T = QUIEROAPRENDERCRIPTOGRAFIA

A continuación, se aplica la permutación fija *PI(T)* conforme lo establecido en la siguiente tabla de permutación:

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 21 | 26 | 24 | 4 | 12 | 8 | 16 | 23 | 7 | 6 | 5 | 15 | 25 |
| 14 | 1 | 19 | 18 | 22 | 20 | 10 | 13 | 9 | 11 | 3 | 2 | 17 |

Con esto, el texto cifrado es el siguiente:

Y = GAFEDPRAAORCIRQTPROEERNIUI

1. **Diga cuál es el conjunto de las llaves .**