



Evaluación de Aprendizaje 2

Temas

Criptografía.

Fechas limites de entregas

| | | |
|------------------------|------------------|--|
| ENTREGA | Lunes 2/11/2020 | Fecha de Entrega |
| DEVOLUCION RDOS | Lunes 9/11/2020 | Fecha Máxima de Devolución de Resultados |
| REENTREGA | Lunes 16/11/2020 | Fecha de Reentrega |

Consigna

Realice los ejercicios planteados a continuación:

1. Cifrador Polybios:

Es el cifrador por sustitución de caracteres más antiguo que se conoce (siglo II a.c.).

El mismo trabaja con una matriz, por lo general cuadrada (en este caso de 5x5), en la cual se colocan los caracteres del alfabeto original.

Para obtener el mensaje cifrado, se busca el par fila/columna y se lo coloca como cifrado. Como puede verse en el gráfico, la letra Q deriva en DA.

Nota: Los espacios en blanco no son tomados en cuenta.

| | A | B | C | D | E | | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| A | A | B | C | D | E | 1 | A | B | C | D | E |
| B | F | G | H | I | J | 2 | F | G | H | I | J |
| C | L | M | N | O | P | 3 | L | M | N | O | P |
| D | Q | R | S | T | U | 4 | Q | R | S | T | U |
| E | V | W | X | Y | Z | 5 | V | W | X | Y | Z |

| | |
|---|---|
| $M_1 = \text{QUÉ BUENA IDEA}$ $C_1 = \text{DA DE AE AB DE AE}$ CC AA BD AD AE EA | $M_2 = \text{LA DEL GRIEGO}$ $C_2 = \text{31 11 14 15 31 22}$ 42 24 15 22 34 |
|---|---|

Se pide:



- Cifrar el mensaje “Seguridad y Calidad en Aplicaciones Web”
- Responder: ¿Qué característica tiene el presente cifrador que lo hace poco interesante para su uso? (sin importar la época histórica)

2. Cifrador Vernam:

En 1917 Gilbert Vernam (MIT) propone un cifrador por sustitución binaria con clave de un único uso, basado en el código Baudot de 5 bits:

La operación de cifrado es la función XOR.

El algoritmo de descifrado es igual al de cifrado por la involución de la función XOR.

La clave será tan larga o más que el mensaje y se usará una sola vez.

Código BAUDOT

| bits | letra | figs | hexa | bits | letra | figs | hexa |
|-------|-------|------|------|-------|-------|------|------|
| 00011 | A | - | 03 | 01100 | N | , | 0C |
| 11001 | B | ? | 19 | 11000 | O | 9 | 18 |
| 01110 | C | : | 0E | 10110 | P | 0 | 16 |
| 01001 | D | \$ | 09 | 10111 | Q | 1 | 17 |
| 00001 | E | 3 | 01 | 01010 | R | 4 | 0A |
| 01101 | F | ! | 0D | 00101 | S | BELL | 05 |
| 11010 | G | & | 1A | 10000 | T | 5 | 10 |
| 10100 | H | STOP | 14 | 00111 | U | 7 | 07 |
| 00110 | I | 8 | 06 | 11110 | V | ; | 1E |
| 01011 | J | ' | 0B | 10011 | W | 2 | 13 |
| 01111 | K | (| 0F | 11101 | X | / | 1D |
| 10010 | L |) | 12 | 10101 | Y | 6 | 15 |
| 11100 | M | . | 1C | 10001 | Z | " | 11 |

Se cifra tomando un carácter del mensaje original y un carácter de la clave y se realiza un XOR. Ejemplo:


$$B \oplus V = 11001 \oplus 11110 = 00111 = U$$

Se pide:

- Cifrar el mensaje "clasesremotas" con la clave "segairdrdyccldidad "

3. Criptoanálisis

Descifrar el siguiente texto: "LZ AHL ZB THW YBL IH XBL KL ILY OH ZLY CH ROK H" por medio de un ataque por características/estadísticas del lenguaje, en nuestro

| | | |
|--|---|--|
| | Evaluación de Aprendizaje Pág. 3 de 3 |  Universidad Nacional de La Matanza |
|--|---|--|

caso el castellano, y teniendo en cuenta el uso intensivo de las vocales “A”, “E”, y “O” del mismo.

Mencionar método de cifrado utilizado y su clave

4. Responda las siguientes preguntas de concepto:

- ¿Cuál de los métodos analizados/utilizados anteriormente le parece más seguro?
- ¿En qué situaciones podrían utilizarse cada uno de estos métodos? (si no fuera conveniente, mencionarlo. No tomar en cuenta la época histórica)
- ¿Cómo serían clasificados cada uno de estos métodos analizados/utilizados en los puntos 1, 2 y 3?
- ¿Qué clase de algoritmo es AES?