Universidad Nacional Autónoma de México
Facultad de Ciencias
Criptografía y Seguridad | 7133
Tarea Corta 1 : | Cifrado afín

Sosa Romo Juan Mario | 320051926

26/08/24

1. **Descifra el siguiente mensaje. Esta hecho con un cifrado afín**

   - Debes mostrar todas las operaciones que hiciste
   - Solo entregar un PDF
   - En caso de querer adjuntar código, en el PDF coloca el link y asegúrate que funcione
   - Puede ser en equipo pero el reporte es individual.

   EM VC FIU TSELMWMI JIXI KH JSKPHC QSK VC FIUI JIB JIXI KH YCPMKXVC

   Desarrollamos y completamos el procedimiento visto en clase

   1. **Planteamos las ecuaciones:**

      $$\begin{aligned} 18\beta + \alpha &\equiv 4 \ mod\ 26 \\ 8\beta + \alpha &\equiv 12 \ mod\ 26 \\ 13\beta + \alpha &\equiv 21 \ mod\ 26 \\ 14\beta + \alpha &\equiv 2 \ mod\ 26 \end{aligned}$$

      Como explicación, estas ecuaciones salen de numerar el alfabeto empezando en a=0 hasta z=25 y de la pista que `SI` se cifro como `EM` y `NO` como `VC`; entonces por ejemplo $S = 18$ & $E = 4 \rightarrow 18\beta + \alpha \equiv 4 \ mod\ 26$.

   2. **Despejamos β utilizando las ecuaciones 3 y 4:**

      Restamos a la 4ta la 3era:

      $$\begin{aligned} (14-13)\beta + (1-1)\alpha &\equiv (2-21) \ mod\ 26 \\ \beta &\equiv -19 \ mod\ 26 \\ \beta &\equiv -19 + 26 \equiv 7 \ mod\ 26 \\ \beta &\equiv 7 \ mod\ 26 \end{aligned}$$

   3. **Despejamos a α utilizando la 2nda ec.**

      Sustituyo el valor de β y resuelvo:

      $$\begin{aligned} 8(7) + \alpha &\equiv 12 \ mod\ 26 \\ 56 + \alpha &\equiv 12 \ mod\ 26 \\ \alpha &\equiv -44 \ mod\ 26 \\ \alpha &\equiv -44 + 26(2) \equiv 8 \ mod\ 26 \\ \alpha &\equiv 8 \ mod\ 26 \end{aligned}$$

4. **Compruebo mis valores utilizando la ec. 1**

   Sustituyo valores y resuelvo:

$$\begin{aligned} 18(7) + (8) &\equiv 4 \ mod\ 26 \\ 126 + 8 &\equiv 4 \ mod\ 26 \\ 134 &\equiv 4 \ mod\ 26 \\ 134\%26 &\equiv 4 \ mod\ 26 \\ 4 &\equiv 4 \ mod\ 26 \end{aligned}$$

   Correcto.

5. **Calculamos inversa para el descifrado:**

   Lo que necesitamos es $\alpha \cdot \alpha^{-1} \equiv 1 \ mod\ 26$, utilizando algoritmo extendido de euclides o probando múltiplos (lo que yo hice con $(7 * n)\%26 = 1$) obtenemos que $a^{-1} = 15$. En el código lo hacemos de manera ingenua.

6. **Creamos código para utilizar esta función letra por letra:**

```python
def decriptar_afin(texto: str, alpha: int, beta: int) -> str:
    """
    Desencripta un texto cifrado con cifrado afin:
    E(x) = alpha*x + beta mod 26

    alpha debe ser coprimo con 26 (para que exista inversa).
    """

    """
    Funcion aux para obtener la inversa modular
    esto prueba valores hasta encontrar el inverso de
    alpha menor a 26
    """
    def modinv(a, m):
        for x in range(1, m):
            if (a * x) % m == 1:
                return x
        raise ValueError(f"No existe inversa modular de {a}
            modulo {m}")

    m = 26
    alpha_inv = modinv(alpha, m)
    texto_descifrado = []

    for ch in texto:
        if 'A' <= ch <= 'Z':
            y = ord(ch) - ord('A')  # conseguimos numeros, rango
                0-25
            x = (alpha_inv * (y - beta)) % m # formulazo
            texto_descifrado.append(chr(x + ord('A'))) #
               regresamos a letra
        else:
            # espacios y signos se dejan igual
            texto_descifrado.append(ch)
```

```
    return ''.join(texto_descifrado)

# ------------------------
# Ejemplo con el caso de la clase
cifrado = "EM VC FIU TSELMWMI JIXI KH JSKPHC QSK VC FIUI JIB
    JIXI KH YCPMKXVC"
alpha = 7
beta = 8

print(f"Texto descifrado:\n {decriptar_afin(cifrado,alpha,beta)}
    ")
```

El código también se encuentra en la siguiente liga: Notebook en colab

Importante recalcar que en Python el comportamiento del modulo % convierte a equivalentes positivos es por eso que el formulazo no muere

7. **Resultado:**

Utilizando el código con lo que hemos encontrado obtenemos el siguiente resultado:

```
Texto descifrado:
 SI NO HAY JUSTICIA PARA EL PUEBLO QUE NO HAYA PAZ PARA EL GOBIERNO
```