Práctica 08. Sistema Criptográfico Mixto: Vigenère y RSA

10 de mayo de 2023

Apellidos: ..... Nombre: .....

Apellidos: ..... Nombre: .....

Grupo G3. Ordenador: .....

En esta práctica vamos a trabajar con un sistema criptográfico mixto, donde los mensajes se cifran usando el sistema de clave privada de Vigenère y la clave privada utilizada se cifra usando el sistema criptográfico de RSA por bloques (sólo podemos intercambiar la clave por el canal, y el canal no es seguro).

Vamos a resolver tres tipos de problemas. El primero consiste en realizar el descifrado de Vigenère, el segundo es el descifrado para el RSA por bloques y el tercero es el descifrado del sistema criptográfico mixto. En los tres problemas a resolver la información está escrita en el alfabeto *alf* formado por los 86 símbolos:

"abcdefghijklmnñopqrstuvwxyzABCDEFGHIJKLMNÑOPQRS
TUVWXYZáéíóúÁÉÍÓÚ0123456789 ,.:!-¿?()"

(alfabeto disponible en la variable alf del fichero entrada_datos_08_G3.txt, dentro de la carpeta práctica 08 de la moodle)

y la codificación numérica del alfabeto asocia a cada símbolo α el número $n(\alpha) = p(\alpha) - 1$, donde $p(\alpha)$ es la posición que ocupa α dentro del alfabeto. Cuando ciframos con RSA, para rellenar el mensaje hasta la longitud apropiada se ha utilizado el mismo padding de la práctica 07.

PROBLEMA 1: Vigenère.

En este caso, el mensaje en claro M se ha cifrado usando el sistema de cifrado de Vigenère con clave de cifrado K (string). Sabiendo que la clave de cifrado es K ="IMMANUEL KANT" y que el mensaje cifrado es el disponible en el fichero *entrada_datos_08_G3.txt*, obtener el mensaje en claro.

10 últimos símbolos de M

PROBLEMA 2: RSA por bloques.

Supongamos que una red local de usuarios utiliza el sistema criptográfico RSA en modo bloques. Se conocen las claves públicas de los usuarios del sistema. Los datos vienen indicados en la tabla siguiente:

usuario	n	e
Benito	71198471775161786826150 79	7654541110992431640625
Pepa	82788920702214745052711	291062977435155133
Juan	962661868537613318993	5791676632597
María	61230685721738457989823 9197	557890978040851

Se pide descifrar el mensaje cifrado que podéis encontrar en *entrada_datos_08_G3.txt*, sabiendo que es un mensaje que María envió a Pepa.

10 últimos símbolos de M

PROBLEMA 3: Sistema Criptográfico Mixto.

En este problema vamos a trabajar con un sistema criptográfico mixto, donde los mensajes se cifran usando el sistema de clave privada de Vigenère y la clave privada utilizada se cifra usando el sistema criptográfico de RSA por bloques. El proceso de cifrado es el siguiente:

- Para enviar el mensaje en claro M al usuario $\mathcal{U}$, se elige una clave K (string) para usarla con Vigenère.
- Ciframos K usando el cifrado RSA por bloques con la clave pública de $\mathcal{U}$. Sea K^* el mensaje cifrado obtenido.
- Ciframos el mensaje M usando la variante de Vigenère con clave privada K. Sea C el mensaje obtenido.
- Enviamos al usuario $\mathcal{U}$ el par (K^*, C).

Se pide descifrar el par cifrado que podéis encontrar en *entrada_datos_08_G3.txt*, sabiendo que es un par que Benito recibe de Juan.

10 últimos símbolos de M