Práctica 7: Simulación de un Sistema Criptográfico Mixto

Mayo de 2021

Supongamos que tenemos un sistema criptográfico mixto, donde los mensajes se cifran usando una variante del sistema de clave privada 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). 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, donde la clave extendida de Vigenère se construye con la ecuación de recurrencia lineal con coeficientes la codificación numérica de la clave K.
- 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

$$(K^*, C).$$

Alicia y Benito son usuarios del sistema y escriben sus mensajes en el alfabeto

$$\mathcal{A} = \text{“ABCDEFGHIJKLMNÑOPQRSTUVWXYZ ÁÉÍÓÚ”}$$

La clave pública para RSA de Alicia es $(n = 21962054407, e = 80263681)$ y la clave pública de Benito es $(n = 9641865053, e = 70241161)$. Se pide:

1. Descifrar el par

$$\Big(\text{ CÉQUANL , EAMGCÍGJKTLÁRMKZÓXÚÉÓQBÓIGÉÍY }\Big)$$

recibido por Alicia.

mensaje en claro

2. Cifrar el mensaje “CADA VEZ QUE CIFRO CAMBIO LA CLAVE” para enviárselo a Benito, usando la palabra “ENIGMA” como clave de Vigenère.

par cifrado