Universidad Nacional Autónoma de México

Facultad de Ciencias

Criptografía y Seguridad

Punto extra.

Fecha de entrega: 23/11/2023

Equipo:

Criptonianos

Acosta Arzate Rubén - 317205776

Bernal Marquez Erick - 317042522

Deloya Andrade Ana Valeria - 317277582

Marco Antonio Rivera Silva - 318183583

(a) En un sistema RSA, interceptas el mensaje C=10, el cuál fue mandado a un usuario cuya llave pública es e=5 y n=35. ¿Cuál es el texto descifrado M?

Primero obtenemos $\phi(35)$, para ello factorizamos $\phi(35) = \phi(7) * \phi(5) = 6 * 4 = 24$

Luego obtenemos $e^{-1} = 5 = d$, pues $5 * 5 \ mod \ 24 = 1$

De esta manera tenemos que $M = 10^5 \ mod \ 35 = 5$

Por lo cual el texto cifrado $M = 5$

(b) En un sistema RSA, la llave pública de un usuario es e=31 y n= 3599. ¿Cuál es la llave privada del usuario?

Primero obtenemos $\phi(3599)$, para ello factorizamos $\phi(3599) = \phi(61) * \phi(59) = 60 * 58 = 3480$

Luego obtenemos $e^{-1} = 3031 = d$, pues $31 * 3031 \ mod \ 3480 = 1$

De esta manera tenemos que $d = 3031$

(c) Usa el algoritmo de exponenciación rápida dado en clase para calcular $5^{596} \ mod \ 1234$**.**

Para ello descomponemos la potencia en sumas

$5^{596} \ mod \ 1234 =$

$5^{256} + 5^{256} + 5^{64} + 5^{16} + 5^4 \ mod \ 1234 =$

$5^{256} + 5^{256} + 5^{16} + 5^{16} + 5^{16} + 5^{16} + 5^{16} + 5^4 \ mod \ 1234 =$

$5^{256} + 5^{256} + 1011 + 1011 + 1011 + 1011 + 1011 + 625 \ mod \ 1234 =$

$5^{256} + 5^{256} + 4044 + 1011 + 625 \ mod \ 1234 =$

De aquí sabemos que $5^{64} \ mod \ 1234 = 4044 = 342 \ mod \ 1234$

$5^{256} + 5^{256} + 5680 \ mod \ 1234 =$

$5^{256} + 5^{256} + 744 \ mod \ 1234 =$

$5^{64} + 5^{64} + 5^{64} + 5^{64} + 5^{64} + 5^{64} + 5^{64} + 5^{64} + 744 \ mod \ 1234 =$

$4044 + 4044 + 4044 + 4044 + 4044 + 4044 + 4044 + 4044 + 744 \ mod \ 1234 =$

$33096 \ mod \ 1234 = 1012$

Por lo cual $5^{596} \ mod \ 1234 = 1012$