Carlos Alberto Gallegos Tena

Examen grupos

Para encriptar el mensaje ORDER A PIZZA. Vamos a separar las letras en 2 y poner una X al final para que nos quede un número par. Entonces tenemos OR DE RA PI ZZ AX. Si los tomamos como números (sin la Ñ) nos queda

O=14 , R=17, D=03, E=04, R=17, A=00, P=15, I=17, Z=25, X=23.

Usando RSA, tenemos la fórmula de encriptación E tal que E(B)=$B^e mod$ n donde B son nuestros números (letras) que queremos encriptar. Entonces, tomando e=5 y n=1459, usando modular exponencial con $5=(101)_2$, tenemos que:

La tabla muestra cómo se calculó el módulo del exponencial correspondiente.

	F	G	H
0	1	1*1417=1417	1417^2 mod 1459=2007889 mod 1459=305
1	0	1417	305^2 mod 1458 = 93025 mod 1459 = 1108
2	1	1417*1108 mod 1459=152	E(B)=152
0	1	304	304^2 mod 1459 = 499
1	0	304	499^2 mod 1459=971
2	1	304*971 mod 1459 = 466	E(B)=466
0	1	1700 mod 1459=241	1700^2 mod 1459=1180
1	0	241	1180^2 mod 1459=514
2	1	241*514 mod 1459=1318	E(B)=1318
0	1	1517 mod 1459=58	1517^2 mod 1459=446
1	0	58	446^2 mod 1459=492
2	1	58*492 mod 1459=815	E(B)=815

$1417^5 mod\ 1459 = 0152$

$0304^5 mod\ 1459 = 0466$

$1700^5 mod\ 1459 = 1318$

$1517^5 mod\ 1459 = 0815$

$2523^5 mod\ 1459 = 0643$

Por lo tanto, el cyphertext para ORDER A PIZZA usando encriptación RSA con e=5 y n=1459 sería 0152

0466 1318 0815 0643.