Matemáticas Discretas II — I Semestre 2023

Parcial # 2 — Profesor: *Rodrigo De Castro K.*

Nombre: [redacted] *Calificación:* 52/60

1. *(20 puntos)* Se ha interceptado un mensaje que ha sido encriptado mediante una transformación afín usando un alfabeto de 26 letras y la siguiente tabla de equivalentes numéricos:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Por análisis de frecuencias se ha determinado que las letras más comunes del español, la E y la A, se han encriptado como G y W, respectivamente. Desencriptar la siguiente porción del mensaje:

DWRQXS.

Presentar el procedimiento completo.

2. *(25 puntos)* Se ha recibido un mensaje encriptado mediante el cifrado exponencial de Diffie-Hellman con clave (p, e), donde p es el primo 2521 y $e = 611$, usando encriptación por digramas y bloques numéricos de máximo cuatro dígitos. Se ha usado la siguiente tabla de equivalentes numéricos para encriptar los digramas:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Desencriptar el siguiente bloque numérico: 447. Presentar el procedimiento completo, incluyendo el cálculo detallado de las potencias módulo m.

3. *(15 puntos)* Considere un criptosistema RSA con primos $p = 71$ y $q = 113$.

(i) Si un usuario tiene clave pública $e = 3267$, ¿cuál es su clave privada?

(ii) Si usuarios distintos tienen claves públicas diferentes (es decir, si no hay claves compartidas) y la clave pública de un usuario no puede ser la clave privada de otro usuario, ¿cuál es el máximo número de usuarios que puede tener la red?

AYUDA: recordar que los valores concretos de la función φ de Euler se pueden calcular mediante las propiedades:

$$\begin{cases} \varphi(mn) = \varphi(m)\varphi(n), & \text{si } \operatorname{mcd}(m,n) = 1, \\ \varphi(p^k) = p^{k-1}(p-1), & \text{si } p \text{ es primo y } k \geq 1. \end{cases}$$

Presentar el procedimiento completo.

① Mensaje encriptado → DWRQXS mod → 26

P C

E(4) ——— G(6)

A(0) ——— W(22)

$C \equiv aP + b \bmod 26$

$P \equiv a^{-1}C - a^{-1}b \bmod 26$ → para desencriptar

① $6 \equiv 4a + b \bmod 26$

② $22 \equiv 0 + b \bmod 26 \rightarrow \boxed{b = 22}$

① reemplazo

$6 \equiv 4a + 22 \bmod 26$

$-16 \equiv 4a \bmod 26$

~~$4a \equiv 10 \bmod 26$~~

$2a \equiv 5 \bmod 13$

$\boxed{a = 9} \rightarrow \boxed{a = 22}$ X

esta sí ✓ — No es invertible

$mcd(4, 26) = 2 \rightarrow$ soluciones ✓

$9x \equiv 1 \bmod 26$

$1 = 9(x) - 26(y)$

$1 = 9 - 8$

$1 = 9 - (26 - 9(2))$

$1 = 9 - 26 + 9(2)$

$1 = 9(3) - 26$ ✓

26 | 9	9 | 8
⑧ 2	① 1

$P \equiv 3C - 3 \times 22 \bmod 26$

$P \equiv 3C - 66 \bmod 26$

$P \equiv 3C + 12 \bmod 26$

"DWRQXS" se desencripta → "Valido"

C	21	P
D(3)		(21) → V
W(22)	78	(0) → A
R(17)		(11) → L
Q(16)		(8) → I
X(23)		(3) → D
S(18)		(14) → O

✓

② Cifrado exponencial clave (p, e), $p=2521$ y $e=611$

desencriptar 447 $D \equiv C^d \bmod p$ · $\text{mcd}(p-1, e)=1$ · $\text{mcd}(2520, 611)=1$

$1 \equiv e(d) - (p-1)(t)$

$1 \equiv 611(x) - 2520(y)$

2520 | 611
2444 | 4
76

611 | 76
608 | 8
3

76 | 3
16 | 25
1

$1 = 76(1) - 3(25)$

$1 = 76(1) - (611 - 76(8))(25)$

$1 = 76(1) - 611(25) + 76(200)$

$1 = 76(201) - 611(25)$

$1 = (2520 - 611(4))(201) - 611(25)$

$1 = 2520(201) - 611(804) - 611(25)$

$1 = 2520(201) - 611(829)$

$d = -829$

$d = 1691$

$(1691)_{10} \rightarrow (11010011011)_2$

$ed \equiv 1 \bmod p-1$

$611(\phi) \equiv 1 \bmod 2520$

$447^{1691} \bmod 2521$

	$v = v \times \square$	mod 2521	Cuadrados	mod 2521
1	447	447	447^2	650
1	447×650	635	650^2	1493
0	~~~	635	1493^2	485
1	635×485	413	485^2	772
1	413×772	1190	772^2	1028
0	~~~	1190	1028^2	485
0	~~~	1190	485^2	772
1	1190×772	1036	772^2	1028
0	~~~	1036	1028^2	485
1	1036×485	781	485^2	772
1	781×772	413	~~~	~~~

413 → M

447 se desencripta → 413 → EN

3) i) $p=71$ y $q=113$, clave pública $e=3267$, privada d_A?

$ed \equiv 1 \bmod \ell(x)$

$3267(d) \equiv 1 \bmod 7840$

$\ell(x) = (p-1)(q-1)$

$= 70 \times 112$

$= 7840$

7840 | 3267
1306 | 2

3267 | 1306
655 | 2

1306 | 655
651 | 1
4 | 3
1

655 | 651
4 | 1

651 | 4
25 | 162
11
3

$1 = 3267(x) - 7840(y)$

$1 = 4 - 3$

$1 = 4 - (651 - 4(162)) \rightarrow 1 = 4(163) - 651$

$1 = (655 - 651)(163) - 651 \rightarrow 1 = 655(163) - 651(164)$

$1 = 655(163) - (1306 - 655)(164)$

$1 = 655(163) - 1306(164) + 655(164) \rightarrow 1 = 655(327) - 1306(164)$

$1 = (3267 - 1306(2))327 - 1306(164) \rightarrow 1 = 3267(327) - 1306(818)$

$1 = 3267(327) - (7840 - 3267(2))(818) \rightarrow 1 = 3267(327) - 7840(818) + 3267(1636) \rightarrow x = 1963$

la clave privada d es (1963)

3) ii)

SOLUCIÓN

$r = p\,q$

$r = 71 * 113$

$r = 8023$

$\phi(p^k) = p^{k-1}(p-1)$

$\phi(r)/2 = \phi(7840)/2$

$\phi(8023) = \phi(71)\,\phi(113)$ → son primos

$= (71-1) * (113-1)$

$= 7840$ → Divido entre 2 por lo que cada usuario tiene su clave pública y privada correspondiente

$mcd(113, 71) = 1$

113 | 71	71 | 42	42 | 29	29 | 13
(42) 1	(29) 1	(13) 1	(3) 2

13 | 3
(1) 4

3920 usuarios máximos que puede tener la red