Name: Chinmai Reg. No: [redacted] Roll No 43

IA 3 Date: 28/10/2025 Marks: 5 M

Subject: Information Security [ICT 3121]

Alice wants to sign a message **M = 45** using the ElGamal Digital Signature Scheme.
Use the following parameters:

- Prime number $p = 211$
- Public base $e_1 = 2$
- Private key $d = 71$
- Random number $r = 23$

Compute all necessary values to generate and verify Alice's digital signature.
Note: Show all intermediate steps clearly.

$M = 45$

Alice

$S1 = e_1^r \% p$

$S2 = (m - dS1) r^{-1} \% (p-1)$

$S1 = 2^{23} \% 211 \quad 23 = 16+4+2+1$

$= 2^1 \times 2^2 \times 2^4 \times 2^{16}$

$2^1 = 2 \% 211$

$2^2 = 4 \% 211$

$2^4 = 16 \% 211$

$2^{16} = 2^8 \times 2^8 = (256 \% 211) \times (256 \% 211)$

$= 45 \times 45$

$= 2025 \% 211$

$= 126$

$S1 = 2 \times 4 \times 16 \times 126 = 41 \times 4 \times 16$

$= 23 \times 4$

$= 92$

$S2 = (45 - 71 \times 92) \times 23^{-1} \% 210$

$= (-6487) \% 210 \times 23^{-1} \% 210$

$= (-6487 \% 210) \times 210$

$= 23 \% 210$

$= 23$

Bob

$c_2 = e_1^d \% p$

$= 2 \times 4 \times 16 \times 69$

$= 64 \times 16 \times 4$

$V_1 = e_1^M \% p$

$V_2 = (e_2^{S1} \times S1^{S2}) \% p$

$V_1 = 2^{45} \% 211$

$45 = 32+8+4+1$

$2 \times 16 \times 45 \times 51$

$= 32 \times 185 = 166$

$V_2 = (92^{24} \times 92^{12}) \% 211$

$= 166$

$\therefore$ Verified.

$T_1 - T_2 Q$

Q	A	B	R	T_1	T_2	T_3
9	210	23	3	0	1	-9
7	23	3	2	1	-9	64
1	3	2	1	-9	64	-73
2	2	1	0	64	-73	210

$1+83 = 210$

$210 \quad 23 \quad 4830$