	1	2	3	4	5	6	7	8	9	1o	11	12	13	14	15	16	17
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	2	4	8	16	9	18	13	3	6	12	1	2	4	8	16	9	18
3	3	9	4	12	13	16	2	6	18	8	1	3	9	4	12	13	16
4	4	16	18	3	12	2	8	9	13	6	1	4	16	18	3	12	2
5	5	2	1o	4	20	8	17	16	11	9	22	18	21	13	19	3	15
6	6	13	9	8	2	12	3	18	16	4	1	6	13	9	8	2	12
7	7	3	21	9	17	4	5	12	15	13	22	16	20	2	14	6	19
8	8	18	6	2	16	13	12	4	9	3	1	8	18	6	2	16	13
9	9	12	16	6	8	3	4	13	2	18	1	9	12	16	6	8	3
1o	10	8	11	18	19	6	14	2	20	16	22	13	15	12	5	4	17
11	11	6	20	13	5	9	7	8	19	2	22	12	17	3	1o	18	14
12	12	6	3	13	18	9	16	8	4	2	1	12	6	3	13	18	9
13	13	8	12	18	4	6	9	2	3	16	1	13	8	12	18	4	6
14	14	12	7	6	15	3	19	13	21	18	22	9	11	16	17	8	20
15	15	18	17	2	7	13	11	4	14	3	22	8	5	6	21	16	1o
16	16	3	2	9	6	4	18	12	8	13	1	16	3	2	9	6	4
17	17	13	14	8	21	12	20	18	7	4	22	6	1o	9	15	2	11
18	18	2	13	4	3	8	6	16	12	9	1	18	2	13	4	3	8
19	19	16	5	3	11	2	15	9	1o	6	22	4	7	18	20	12	21
2o	20	9	19	12	1o	16	21	6	5	8	22	3	14	4	11	13	7
21	21	4	15	16	14	18	1o	3	17	12	22	2	19	8	7	9	5
22	22	1	22	1	22	1	22	1	22	1	22	1	22	1	22	1	22

Primitive Root of 23	5	7	10	11	14	15	17	19	20	21

Q	23	α	5	Public Values
Sender		Reciver		
Va	6	Vb	3	Private Values
Ka	8	Kb	10	Public Values
P	6	P	6	Reverse Values

18	19	2o	21	22
1	1	1	1	1
13	3	6	12	1
2	6	18	8	1
8	9	13	6	1
6	7	12	14	1
3	18	16	4	1
18	11	8	1o	1
12	4	9	3	1
4	13	2	18	1
9	21	3	7	1
16	15	4	21	1
16	8	4	2	1
9	2	3	16	1
4	1o	2	5	1
12	19	9	20	1
18	12	8	13	1
3	5	16	19	1
6	16	12	9	1
8	14	13	17	1
2	17	18	15	1
13	20	6	11	1
1	22	1	22	1