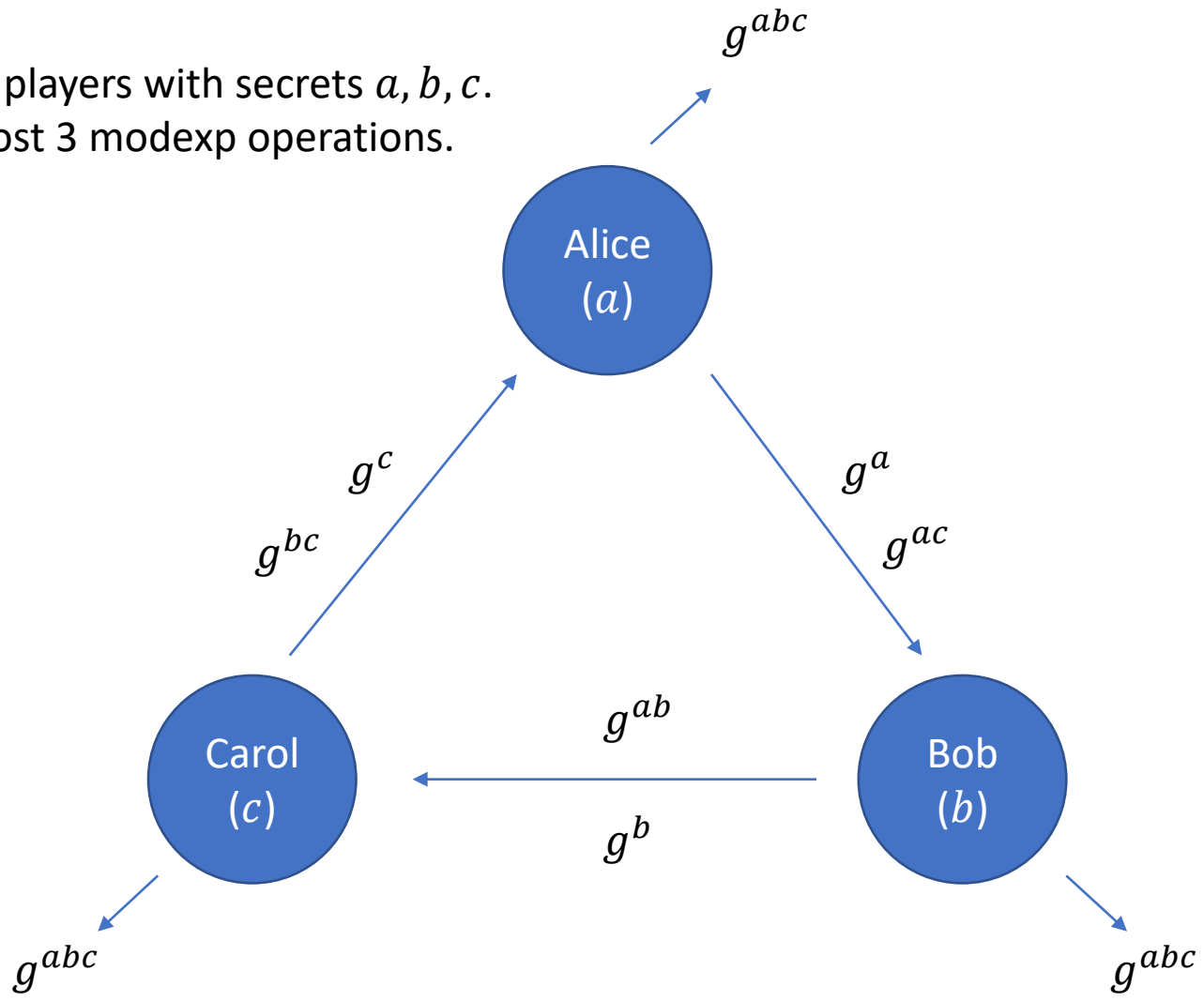
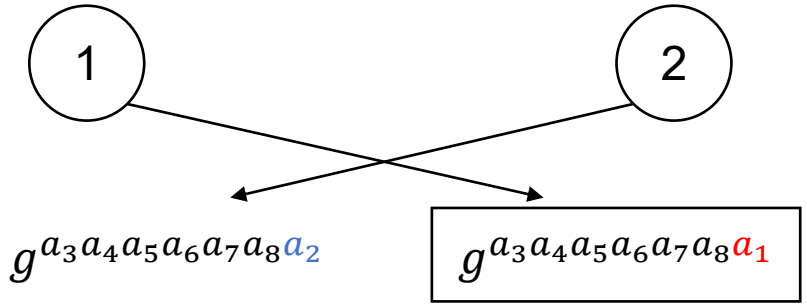
Implement a protocol for three players with secrets a, b, c.
Each player must perform at most 3 modexp operations.



1. איזה הודעה ישלח משתתף 1 ל-2 בשלב השלישי (והאחרון)?



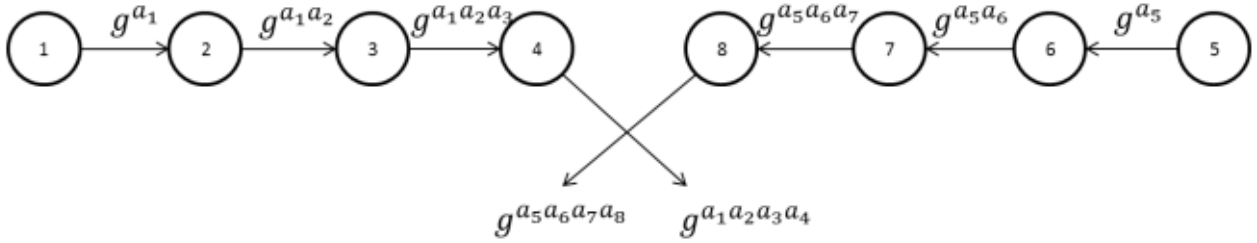
2. איזו פעולה יעשה משתתף 2 לאחר השלב השלישי, כדי לחשוף את הסוד המשותף?

משתתף 2 יעלה בחזקת a_2 את ההודעה שקיבל מ-1:

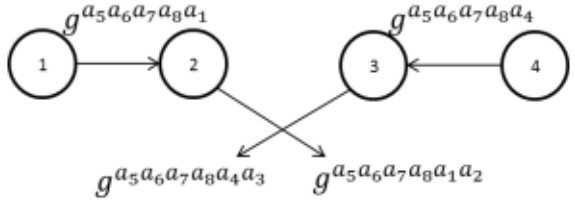
$$(g^{a_3a_4a_5a_6a_7a_8a_1})^{a_2} = g^{a_1a_2a_3a_4a_5a_6a_7a_8}$$

ג. להלן תיאור של פרוטוקול מורחב עבור N=8 משתתפים. נסמן את הסוד הפרטי של משתתף i ב-a_i.

שלב 1: מחלקים את המשתמשים ל- 2 קבוצות שוות, ושולחים את ההודעות הבאות:



שלב 2: מחלקים כל קבוצה באופן דומה וחוזרים על התהליך, כאשר בכל קבוצה ההודעה ההתחלתית היא ההודעה שנשלחה בסוף השלב הקודם מהקבוצה השנייה. למשל, משתתפים 1, 2, 3 ו- 4 מחולקים שוב וחוזרים על התהליך, עם ההודעה ההתחלתית $g^{a_5a_6a_7a_8}$:



3. מהו הסוד המשותף לכל 8 המשתתפים?

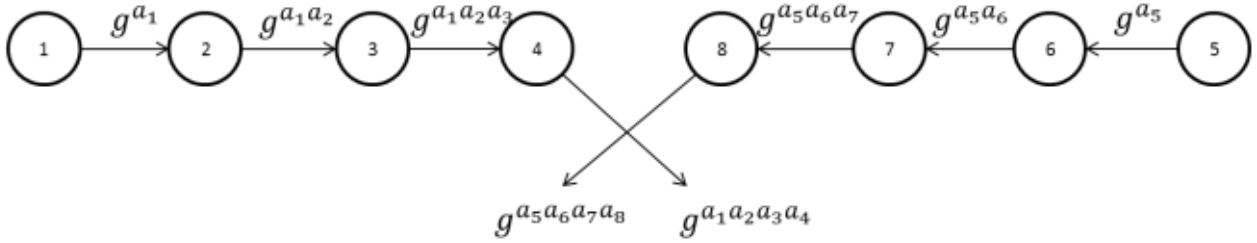
$$g^{a_1 a_2 a_3 a_4 a_5 a_6 a_7 a_8}$$

4. עבור N משתתפים, כמה פעולות modular exponentiation מבצע כל משתתף? יש לתת תשובה במונחים של O, הדוקה ככל שניתן.

- $logN$ שלבים בפרוטוקול
- בכל שלב כל משתתף מבצע פעולה אחת של modular exponentiation
- עוד חישוב אחד בסוף לקבל הסוד המשותף
- סך הכל $O(logN)$ פעולות

ג. להלן תיאור של פרוטוקול מורחב עבור N=8 משתתפים. נסמן את הסוד הפרטי של משתתף i ב-a_i.

שלב 1: מחלקים את המשתמשים ל- 2 קבוצות שוות, ושולחים את ההודעות הבאות:



שלב 2: מחלקים כל קבוצה באופן דומה וחוזרים על התהליך, כאשר בכל קבוצה ההודעה ההתחלתית היא ההודעה שנשלחה בסוף השלב הקודם מהקבוצה השנייה. למשל, משתתפים 1, 2, 3 ו- 4 מחולקים שוב וחוזרים על התהליך, עם ההודעה ההתחלתית $g^{a_5 a_6 a_7 a_8}$: