

## מפתחות סימטריים סודיים

בעולם האמיתי זה קשה, ארוך ומסובך להצפין א-סימטרית הודעות ארוכות, לכן אפשר לעבוד עם הצפנות סימטריות שידועות רק לשני הצדדים. כיצד עושים זאת?

איך להעביר מפתח סימטרי?  
2 שיטות.

1. על ידי הצפנה של המפתח הסימטרי בעזרת RSA ושליחת המסר המוצפן.

2. אלגוריתם Diffie-Helman

מבוסס על בחירת שני ראשוניים ששני הצדדים (וכל העולם) יודעים עליהם, למשל  
 $g=29$   
 $p=17$

כעת כל צד יבחר מפתח פרטי משלה ללא הגבלת הכלליות, נניח שבוב בחר 6  
ואליס בחרה 15.

הפעולה שכל אחד יעשה זה להעלות את המפתח הפרטי שבחר/ה בחזקת  $g$   
מודולו  $p$ .

את התוצאה יחליפו ביניהם. בדוגמה הזאת:

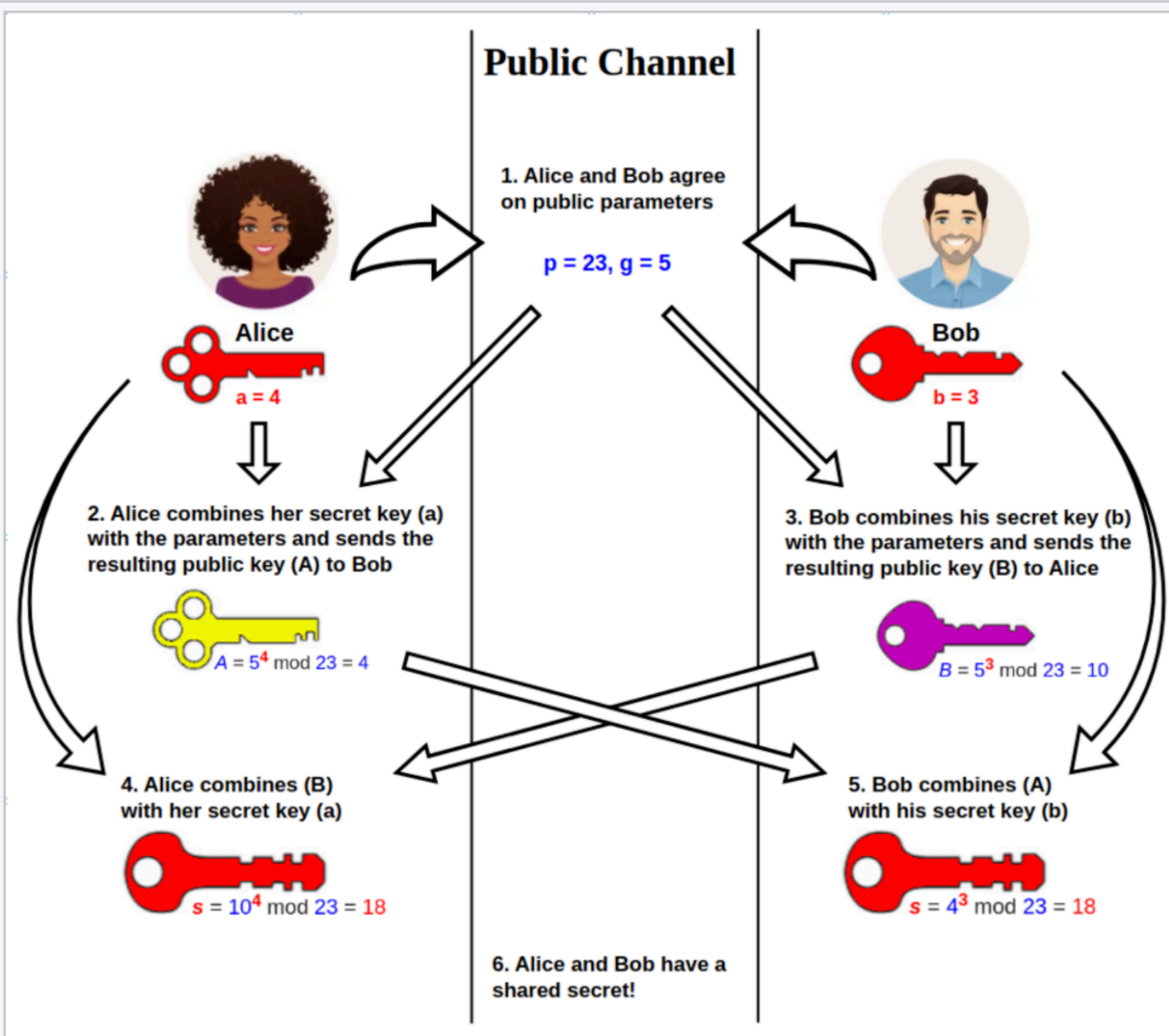
Bob:  $29^6 \pmod{17} = 2$   
Alice:  $29^{15} \pmod{17} = 10$

אליס שולחת לבוב 10 ובוב שולח לאליס 2.

כעת כל אחד יקח את התוצאה של האחר, יעלה בחזקת המפתח הפרטי שבחר/ה  
מודולו  $p$

Bob:  $10^6 \pmod{17} = 9$   
Alice:  $2^{15} \pmod{17} = 9$

לכן שניהם הגיעו למפתח משותף, 9 במקרה זה, שידוע רק להם (כי את המפתחות הפרטיים הם המציאו לבדם ולא העבירו ביניהם).



With Diffie–Hellman key exchange, two parties arrive at a common secret key, without passing the common secret key across the public channel.