מבוא להצפנה: תרגיל 5

חוץ משאלה 2, wolframalpha מספיק כדי לפתור את השאלות. לשאלה 2, צריך להשתמש בטבלת אקסל או לכתוב קוד קצר.

1. לאליס יש מפתח ציבורי $(n,e)=(168163,17)$ להצפנה ב-RSA. המפתח הסודי שלה הוא 59057. השתמשו בנתונים האלה כדי לפרק את n.
2. השתמשו באלגוריתם rho של פולארד כדי לפרק את 168163.
3. השתמשו באלגוריתם p-1 של פולארד כדי לפק את 168163.
4. השתמשו באלגוריתם של פרמה כדי לפרק את 168163.
5. השתמשו בשיטה "בסיס גורמים" כדי לפרק את 168163.
6. פרקו את המספרים $3077^2, 8077^2, 9398^2, 1964^2, 7078^2, 19095^2, 14262^2 \bmod 3837523$ והשתמשו בזהויות שמצאתם כדי לפרק את 3837523.

בהצלחה!