1. $m_1 \equiv_p m_p$ -! $m_1 \equiv_q m_q$

2. $m_2 \equiv_p -m_p$ -! $m_2 \equiv_q -m_q$

3. $m_3 \equiv_p m_p$ -! $m_3 \equiv_q -m_q$

4. $m_4 \equiv_p -m_p$ -! $m_4 \equiv_q m_q$

נסתכל על (m_p, m_q), $(m_p, -m_q)$, $(-m_p, m_q)$, $(-m_p, -m_q)$
מילדה בשביל סיבוכיות לכל הפירוק p,q. נסתכל ב- ההודעות
$m_1, \dots, m_4$ בהסתברות. אחד מהם ← ההודעה.

משפט: נניח שיש אלגוריתם A שבהינתן הצפנה c מחזיר את $m_1, \dots, m_4$
אז יש אלגוריתם A' שבהינתן n מוכלל p,q.

הוכחה: אלגוריתם A' קלט n, פלט p,q.

1. נבחר $0<x<n$ ונחשב $\gcd(x,n)$ אם הוא לא 1
אז הצלחנו לפרק.
2. נצפין את x, $c=x^2 \bmod n$
3. נריץ על A את x ונקבל m.
4. נחשב $\gcd(m-x,n)$ אם הוא לא 1 או n אז סיימנו
אחרת נחזור על האלגוריתם.

נראה שההסתברות $\geq \frac{1}{2}$ מוצאים p,q. אם בשלב 1 מצאנו הצלחה
ניח $\gcd(x,n)=1$. אינו יכולים ש $x^2 \equiv_{pq} m^2$

יש ארבע אפשרויות:

1. $m \equiv_p x \wedge m \equiv_q x$
2. $m \equiv_p -x \wedge m \equiv_q -x$
3. $m \equiv_p x \wedge m \equiv_q -x$
4. $m \equiv_p -x \wedge m \equiv_q x$

ניח קרה ב. אז $p \mid m-x$ אבל $q \nmid m-x$ כי
$q \mid m+x$ כי אם ניח ש $q \mid m-x$ אז $m+x \equiv_q m-x$
ואז נקבל בעיה $x \equiv_q -x$ זה ומשמעות זה את $x=0$