יישום נוסף אפשרי: כריית שורשים: מציאת הפתרון ל- $x^m (mod\ n)$

משפט: אם יש שורש פרימיטיבי מודולו n ו-a זר ל-n אז לקונגרואנציה $x^m \equiv a (mod\ n)$ יש פתרון אמ"מ

$$a^{\frac{\phi(n)}{gcd(m,\phi(n))}} \equiv 1 \ (mod\ n)$$

ואז יש $gcd(m,\phi(n))$ פתרונות.

הוכחה: בתרגיל הבית.

שיטות הצפנה קשורות למספרים ראשוניים.

שיטת RSA: ([illegible])

אריך יבחר n ו-m ויכתוב. בק [illegible] n, m. אריך, רוצה שיעביר הודעה A (שהיא מספר שלם קטן מ-$\underbrace{n}_{\text{זר ל-}n}$). הוא משדר:

$$A^m (mod\ n)$$

המס' s נבחר רק כ- $m \cdot s \equiv 1 (mod\ \phi(n))$

בוב מפענח:

$$(A^m)^s \equiv A^{ms} \equiv A (mod\ n)$$

באופן מעשי ניקח את n להיות מכפלה של 2 ראשוניים, נגיד עם 100 ספרות כל אחד.

עובדה מעניינת: גם אם (n,m) מפורסמים בפומבי עדיין קשה למצוא (שאינו ידוע אחד) לפענח אף אחד לא יכול לפענח.

אם $n=pq$, p,q ראשוניים, אז $\phi(n)=(p-1)(q-1)$ וכל מי שיבחר את p,q יכול לחשב את $\phi(n)$, אבל מי שיודע רק את n יתקשה, מאחר ואין דרך למצוא את p,q כדי לקבל את $\phi(n)$ ולכן לבצע החישוב ולמצוא את s מתוך (n,m)

מסקנה: בוב יודע את (n,s), ויש לו $A^m (mod\ n)$ ולכן יוכל לפענח על ידי חישוב $(A^m)^s (mod\ n)$

שיטת דיפי-הלמן לתיאום מפתחות

אליס ובוב מספרים זה לזה ראשוני p ו-a זר ל-p (ידועים לכל).

אליס, בוחר $0<k_a<p-1$ סודי ומשדר $a^{k_a} \pmod p$.

בוב בוחר $0<k_b<p-1$ סודי ומשדר $a^{k_b} \pmod p$,

הסוד המשותף: $a^{k_a k_b} \pmod p$

$$(a^{k_a})^{k_b} = (a^{k_b})^{k_a}$$

לא ידועה דרך יעילה מידיעת a, p ו-$a^k \pmod p$ לגלות את k (בעיית הלוגריתם הבדיד)

יעיל: $a, p, k \rightarrow a^k \pmod p$

לא יעיל: $a, p, a^k \pmod p \rightarrow k$