Definisjoner

1 Kvadratfrie tall

Et naturlig tall n er kvadratfritt hvis det ikke finnes noe primtall p slik at $p^2 \mid n$

Eks: $42 = 2 \cdot 3 \cdot 7$ er kvadratfritt

$44 = 2^2 \cdot 7$ er ikke kvadratfritt da $2^2 \mid 44$

Formel: Hvis n er kvadratfritt er

$a^{\varphi(n)+1} \equiv a \pmod{n}$ og

$a^{x \cdot \varphi(n)+1} \equiv a \pmod{n}$

Oppskrift

1 Modulere potenser for kvadratfrie m

- Sjekk at m er kvadratfri
- Regn ut $\varphi(m)$
- Bruk at $a^{\varphi(m)+1} \equiv a \pmod{m}$

Eks: $18^{867} \pmod{42}$

42 er kvadratfritt da det er $42 = 2 \cdot 3 \cdot 7$

$\varphi(42) = \varphi(2) \cdot \varphi(3) \cdot \varphi(7) = 1 \cdot 2 \cdot 6 = 12$

$18^{c \cdot \varphi(m)+1} \equiv 18 \pmod{m}$

$18^{867} = 18^{72 \cdot 12 + 3} = 18^{72 \cdot 12 + 1} \cdot 18^2 = 18 \cdot 18^2 \equiv 36 \pmod{42}$

2 RSA

- Velg to hemmelige primtall p og q
- Setter offentlig tall $n = p \cdot q$
- Velger offentlig krypteringseksponent e Merk: $e \perp \phi(N)$
- Regner ut d (dekrypteringseksponent)

  $e \cdot d \equiv 1 \pmod{\phi(N)}$ -> Euclids utvidete algoritme

- Kryptert melding c : $c \equiv m^e \pmod{N}$
- Dekryptert melding m : $m \equiv c^d \pmod{N}$