TU/e Technische Universiteit Eindhoven University of Technology

M-RSA

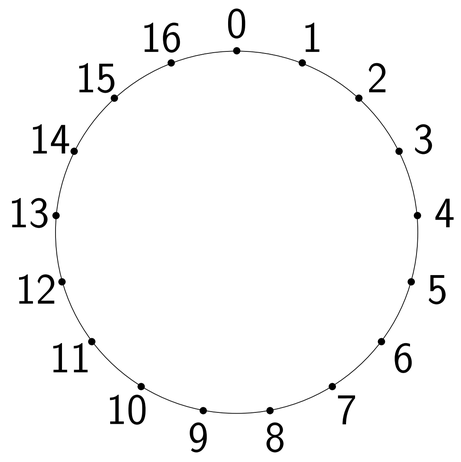
Crypto Werkplaats: Cryptografie met publieke sleutels

1. Modulo 12 rekenen

Analogie: Als het 2 uur is, dan is het over 12 uur weer 2 uur. Over 30 uur is het dan 8 uur.
In beide gevallen beginnen we na 12 uur opnieuw te tellen. Dit heet modulo 12 rekenen.

Bij rekenen modulo 12 werken we met de getallen $0, 1, 2, 3, \ldots, 10, 11$.
Alle veelvouden van 12 zijn voor ons 0.

2. Modulo 17



Afspraak: Als we modulo 17 rekenen gebruiken we $\equiv$ en schrijven we er mod 17 achter.
B.v. $8 + 13 \equiv 21 \bmod 17 \equiv 4 \bmod 17$.

3. Sleutels

- Anita kiest twee gehele getallen en noemt ze a en b.
- Anita berekent $M = a \cdot b - 1$.
- Anita kiest verder twee gehele getallen a' en b' en berekent
$$e = a' \cdot M + a,$$
$$d = b' \cdot M + b,$$
$$n = (e \cdot d - 1)/M.$$
- De publieke sleutel is (n, e).
- De geheime sleutel is d.

Opgave: Laat zien dat n een geheel getal is.

4. Voorbeeld (1)

- Anita kiest $a = 3$ en $b = 4$ en berekent
$M = a \cdot b - 1 = 3 \cdot 4 - 1 = 11$.
- Verder kiest Anita $a' = 2$ en $b' = 3$ en berekent
$e = 2 \cdot 11 + 3 = 25$,
$d = 3 \cdot 11 + 4 = 37$,
$n = (25 \cdot 37 - 1)/11 = 84$.
- De publieke sleutel is $(n, e) = (84, 25)$.
- De geheime sleutel is $d = 37$.

5. Versleutelen

- Benne kent de publieke sleutel van Anita, namelijk n en e.
- Benne kan Anita een getal m (dus een bericht) sturen met behulp van haar publieke sleutel (n, e).
- Benne berekent het geheimschrift
$$c \equiv e \cdot m \bmod n$$
- Benne stuurt de cijfertekst c naar Anita.

6. Voorbeeld (2)

- Benne wil Anita het getal $m = 13$ sturen:
- Benne berekent het geheimschrift
$$c = 73 \equiv 25 \cdot 13 \bmod 84$$
- Benne stuurt de cijfertekst 73 naar Anita.

7. Ontcijferen

- Anita ontvangt het geheimschrift c en kan nu haar geheime sleutel gebruiken om m te ontcijferen.
- Ze ontsleutelt het oorspronkelijke bericht door c met d te vermenigvuldigen (modulo n).

8. Voorbeeld (3)

- Anita kan $m = 73$ met behulp van haar geheime sleutel $d = 37$ ontcijferen:
$$\begin{aligned} c \cdot d &\equiv 73 \cdot 37 \bmod 84 \\ &\equiv 2701 \bmod 84 \\ &\equiv 13 \bmod 84. \end{aligned}$$

9. Opgaven

- Waarom krijgt Anita het oorspronkelijke bericht terug? Leg uit waarom
$$m \equiv d \cdot c \bmod n$$
geldt.
- Kies een publieke en geheime sleutel en versleutel je eigen bericht.
- Kun je dit systeem kraken?

Zie ook: Neil Koblitz, "Cryptography As a Teaching Tool" in Cryptologia, Vol. 21, No. 4 (1997).
`http://www.math.washington.edu/~koblitz/crlogia.html`