RSA

Schemat ogólny:

1. Wybieramy dwie liczby pierwsze "p" i "q"
2. Obliczamy "n" $n = p \cdot q$
3. Obliczamy $\varphi(n)$ [funkcja Eulera] $\varphi(n) = (p-1)(q-1)$
4. Wybieramy liczbę "e" według zasad:
   a) $1 < e < n$
   b) nieparzysta
   c) względnie pierwsza do $\varphi(n)$ $\Rightarrow NWD(e, \varphi(n)) = 1$
   d) nie musi być liczbą pierwszą
5. Obliczamy "d" $d \cdot e \equiv 1 \mod \varphi(n)$
6. Tworzymy klucz publiczny (e, n)
7. Tworzymy klucz prywatny (d, n)
8. Szyfrujemy $m' = m^e \mod n$
9. Deszyfrujemy $m = (m')^d \mod n$

PRZYKŁAD RSA

1) $p = 7 \quad q = 11$

2) $n = p \cdot q = 7 \cdot 11 = 77$

3) $\varphi(n) = (p-1)(q-1) = (7-1)(11-1) = 6 \cdot 10 = 60$

4) $e = 13$ spr.
$60 = 13 \cdot 4 + 8$
$13 = 8 \cdot 1 + 5$
$8 = 5 \cdot 1 + 3$
$5 = 3 \cdot 1 + 2$
$3 = 2 \cdot 1 + 1$
$2 = 1 \cdot 2 + 0$

5) $d \cdot e \equiv 1 \mod \varphi(n)$

$d \cdot 13 \equiv 1 \mod 60$

$d \cdot 13 \equiv 3 - 2 \cdot 1 \mod 60$

$d \cdot 13 \equiv 3 - (5 - 3 \cdot 1) \cdot 1 \mod 60$

$d \cdot 13 \equiv 3 - 5 + 3 \cdot 1 \mod 60$

$d \cdot 13 \equiv 3 \cdot 2 - 5 \mod 60$

$d \cdot 13 \equiv (8 - 5 \cdot 1) \cdot 2 - 5 \mod 60$

$d \cdot 13 \equiv 8 \cdot 2 - 5 \cdot 2 - 5 \mod 60$

$d \cdot 13 \equiv 8 \cdot 2 - 5 \cdot 3 \mod 60$

$d \cdot 13 \equiv 8 \cdot 2 - (13 - 8 \cdot 1) \cdot 3 \mod 60$

$d \cdot 13 \equiv 8 \cdot 2 - 13 \cdot 3 + 8 \cdot 3 \mod 60$

$d \cdot 13 \equiv 8 \cdot 5 - 13 \cdot 3 \mod 60$

$d \cdot 13 \equiv (60 - 13 \cdot 4) \cdot 5 - 13 \cdot 3 \mod 60$

$d \cdot 13 \equiv 60 \cdot 5 - 13 \cdot 20 - 13 \cdot 3 \mod 60$

$d \cdot 13 \equiv 60 \cdot 5 - 13 \cdot 23 \mod 60$

$d \cdot 13 \equiv -13 \cdot 23 \mod 60 \quad // \; 60 \cdot 5 \mod 60 = 0$

$d \cdot 13 \equiv -13 \cdot 23 \mod 60 \quad /: 13$

$d \equiv -23 \mod 60$

$d = 37 \quad // \; 60 - 23 = 37$

6) $(e, n) = (13, 77)$

7) $(d, n) = (37, 77)$

8 i 9) Na stronie szyfrowanie / deszyfrowanie powiadomienia

RSA - szyfrowanie / deszyfrowanie

- M - powiadomienia $(m_1, m_2, \dots, m_n)$ ← [bloki tej samej długości]
- Szyfrowanie $C = c_1, c_2, \dots, c_n$

  $c_i = (m_i)^e \bmod n$ // klucz publiczny
- Deszyfrowanie $\hat{m} = (c_i)^d \bmod n$ // klucz prywatny
- Przykład

  $m = $ 'B A C'
  ↓ ↓ ↓
  2 1 3

  klucz publiczny: (7, 33)
  klucz prywatny: (3, 33)

  $e = 7$
  $d = 3$
  $n = 33$

- szyfrowanie

  $c_1 = (2)^7 \bmod 33 = 128 \bmod 33 = 29$

  $c_2 = (1)^7 \bmod 33 = 01$ // dopisujemy zero przed każdą liczbą od 1 do 9

  $c_3 = (3)^7 \bmod 33 = 2187 \bmod 33 = 9 = 09$

  $C = 290109$

- deszyfrowanie

  $m_1 = (29)^3 \bmod 33 = 24389 = 2 \Rightarrow B$

  $m_2 = (01)^3 \bmod 33 = 1 \Rightarrow A$

  $m_3 = (09)^3 \bmod 33 = 729 \bmod 33 = 3 \Rightarrow C$

  $\hat{M} = B\ A\ C$