1 Algorytm szyfrowania RSA

Na początku generujemy dla siebie parę kluczy (publiczny i prywatny) w następujący sposób.

1. Wybieramy $p \neq q$: duże liczby pierwsze.
2. Obliczamy $n = p \cdot q$.
3. Znajdujemy dużą liczbę d względnie pierwszą z $(p-1) \cdot (q-1)$.
4. Znajdujemy takie e, że $d \cdot e \mod (p-1) \cdot (q-1) = 1$ (za pomocą rozszerzonego algorytmu Euklidesa).
5. Para (e, n) to nasz klucz publiczny, a (d, n) to nasz klucz prywatny.

2 Szyfrowanie wiadomości

Jak zaszyfrować wiadomość? Zapisujemy ją bitowo i dzielimy na kawałki, których długość jest nie większa od $\log n$. Dzięki temu każdy z kawałków jest liczbą z zakresu $[0, n)$. Każdą z liczb będziemy szyfrować osobno.[1]

Załóżmy zatem, że chcemy zaszyfrować liczbę $m \in [0, n)$. Obliczamy liczbę

$$E(m) = m^e \mod n \ ,$$

i wysyłamy ją jako szyfrogram s odbiorcy. Odbiorca otrzymuje szyfrogram s i odszyfrowuje go obliczając

$$D(s) = s^d \mod n \ .$$

[1] Takie naiwne podejście prowadzi do tego, że takie same kawałki byłyby szyfrowane w ten sam sposób. W praktyce stosuje się różne obejścia tego problemu, np. dołączanie losowego ciągu.

3 Poprawność

Musimy pokazać, że dla dowolnego $m \in [0, n)$ zachodzi $D(E(m)) = m$. Przekształcając otrzymujemy

$$\begin{aligned} D(E(m)) &= (m^e \mod n)^d \mod n \\ &= (m^e)^d \mod n && \text{(z własności modulo)} \\ &= m^{k\cdot(p-1)\cdot(q-1)+1} \mod n. && \text{(gdzie } k \in \mathbb{N} \cup \{0\}) \end{aligned}$$

Chcemy teraz pokazać, że $m^{k(p-1)\cdot(q-1)+1} \equiv m \mod n$.

Dla m względnie pierwszych z n, możemy zastosować bezpośrednio twierdzenie Eulera (patrz poniżej), żeby uzyskać

$$m^{k(p-1)\cdot(q-1)+1} \mod n = (m^{(p-1)\cdot(q-1)})^k \cdot m \mod n = 1^k \cdot m \cdot n = m.$$

4 Poprawność, cd.

Dla dowolnej wartości m, możemy argumentować następująco. Obliczmy najpierw wartość $m^{k\cdot(p-1)\cdot(q-1)+1} \mod p$.

- Jeśli $m \mod p = 0$, to $m^{k(p-1)\cdot(q-1)+1} \mod p = 0 = m \mod p$.
- Jeśli natomiast $m \mod p \neq 0$, to $m = \ell \cdot p + m_p$, gdzie $\ell \in \mathbb{N} \cup \{0\}$ i $0 < m_p < p$. Wtedy

$$\begin{aligned} m^{p-1} \mod p &= (\ell \cdot p + m_p)^{p-1} \mod p \\ &= m_p^{p-1} \mod p \\ &= 1. \qquad \text{(z twierdzenia Eulera)} \end{aligned}$$

Stąd $m^{k\cdot(p-1)\cdot(q-1)+1} \mod p = 1^{k\cdot(q-1)} \cdot m \mod p = m \mod p$.

W analogiczny sposób otrzymujemy również, że $m^{k\cdot(p-1)\cdot(q-1)+1} \equiv m \mod q$. Łącząc te dwie równości za pomocą chińskiego twierdzenia o resztach otrzymujemy $m^{k\cdot(p-1)\cdot(q-1)+1} \equiv m \mod pq$.

5 Twierdzenie Eulera

Twierdzenie 5.1 (Twierdzenie Eulera)**.** *Dla dowolnej dodatniej liczby naturalnej n, niech $\mathbb{Z}_n^* = (\{a : 1 \leqslant a \leqslant n \wedge a \perp n\}, \cdot \mod n)$ będzie grupą, której elementami są liczby względnie pierwsze z n, zaś działaniem mnożenie modulo n. Niech $\phi(n)$ będzie liczbą elementów takiej grupy. Wtedy dla $m \in \mathbb{Z}_n^*$ zachodzi $m^{\phi(n)} \equiv 1 \mod n$.*