RSA

- Witfield Diffie i Martin Hellman — idea kryptografii z kluczem publicznym, rok 1976
- RSA — Ron Rivest, Adi Shamir i Leonard Adleman, rok 1978
- bezpieczeństwo algorytmu RSA opiera się na trudności obliczeniowej związanej z rozkładem dużych liczb na czynniki (faktoryzacja)

  Wybierzmy dwie duże liczby pierwsze p i q i obliczmy ich iloczyn (iloczyn łatwo obliczyć)

  $$n = pq,$$

  następnie wybierzmy losowo liczbę e < n względnie pierwszą

  z liczbą $(p - 1)(q - 1)$. Liczba e będzie kluczem szyfrującym.

RSA

Teraz znajdźmy liczbę *d* taką, że

$$ed \equiv 1 \ (mod \ (p-1)(q-1))$$

lub inaczej

$$d \equiv e^{-1} \ (mod \ (p-1)(q-1))$$

Liczby *d* i *n* są także względnie pierwsze. Do obliczenia *d* można użyć rozszerzonego algorytmu Euklidesa. Liczba *d* jest kluczem deszyfrującym. Liczby {*e, n*} stanowią klucz publiczny, który ujawniamy, zaś liczby {*d, n*} stanowią klucz prywatny, który powinien być ściśle chroniony (liczba *d*)

RSA – szyfrowanie i deszyfrowanie

- **Szyfrowanie**

Wiadomość dzielimy na bloki m_i mniejsze niż n, które szyfrujemy używając formuły

$$c_i \equiv m_i^e \pmod{n}$$

- **Deszyfrowanie**

Tekst jawny z kryptogramu otrzymujemy obliczając

$$m_i \equiv c_i^d \pmod{n}$$

RSA – szyfrowanie i deszyfrowanie

Uzasadnienie

Ponieważ $ed \equiv 1 \pmod{(p-1)(q-1)}$,

to istnieje liczba całkowita k taka, że

$$ed = 1 + k(p-1)(q-1).$$

Z małego twierdzenia Fermata, dla NWD(m, p) = 1, mamy:

$$m^{p-1} \equiv 1 \pmod{p}$$

podnosząc obie strony tej kongruencji do potęgi $k(q-1)$ oraz mnożąc przez m otrzymujemy:

$$m^{1+k(p-1)(q-1)} \equiv m \pmod{p}$$

RSA – szyfrowanie i deszyfrowanie

Kongruencja ta jest także prawdziwa dla NWD(m, p) = p, ponieważ wtedy obie strony przystają do 0 (mod p). Zatem, zawsze mamy:

$$m^{ed} \equiv m \pmod{p}$$

Podobnie,

$$m^{ed} \equiv m \pmod{q},$$

a ponieważ p i q są rożnymi liczbami pierwszymi, to z chińskiego twierdzenia o resztach otrzymujemy

$$m^{ed} \equiv m \pmod{n}$$

RSA – przykład

Znajdowanie klucza:

$p = 1123$ $q = 1237$

$n = pq = 1389151$

$\phi = (p - 1)(q - 1) = 1386792$

$e = 834781$

$d \equiv e^{-1} \pmod{\phi} = 1087477$

Szyfrowanie:

$m = 983415$

$c \equiv m^e \pmod{n}$

$983415^{834781} \pmod{1389151} = 190498$

Deszyfrowanie:

$m \equiv c^d \pmod{n}$

$190498^{1087477} \pmod{1389151} = 983415$