ABSTRAK

SISTEM PENYANDIAN RSA

Dalam tulisan ini disajikan sistem penyandian yang dirancang pada tahun 1977 oleh Rivest, Shamir dan Adleman, dan dikenal dengan nama "Sistem Penyandian RSA".

Dalam sistem penyandian ini, pengirim dan penerima pesan memilih dua buah bilangan prima p dan q yang berbeda dan dirahasiakan, serta sebuah bilangan bulat a yang prima relatif terhadap (p-1)(q-1), di mana $0 < a < (p-1)(q-1)$. Bilangan a dan $n = pq$ tidak perlu dirahasiakan.

Dengan menggunakan suatu tabel yang telah disepakati, pesan yang akan dikirimkan diubah ke dalam bentuk desimal menjadi barisan bilangan bulat $M_i$ di mana $0 < M_i < n$.

Pesan yang dikirimkan adalah barisan bilangan bulat $R_i$, yang didapat dari persamaan $R_i \equiv M_i^a \pmod{n}$.

Untuk membaca pesan sandi tersebut si penerima pesan harus menghitung invers dari a, namakan d, dalam modulo (p-1)(q-1), yaitu $ad \equiv 1 \pmod{(p-1)(q-1)}$. Masing-masing $M_i$ diperoleh dari persamaan $M_i \equiv R_i^d \pmod{n}$. Barisan bilangan bulat $M_i$ dibaca dengan menggunakan tabel yang sama.