ABSTRAKSI

Implementasi algoritma enkripsi data (payload) pada suatu chip yang ditetapkan dalam spesifikasi Bluetooth merupakan desain yang lebih komplek dari generasi sebelumnya yaitu Data Encryption Standard. Bluetooth mensyaratkan bahwa hanya data pengguna yang dienkripsi, sedang packet header maupun access code tidak. Plain-text masukan merupakan suatu serial bit stream, yang di-encode-kan secara penjumlahan mod-2 dengan suatu key stream yang dibangkitkan pada chip. Keluaran chipper-text berupa encoded serial bit stream. Fungsi logic pada chip ini, yang paling banyak yaitu ditujukan untuk membangkitkan serial key stream.