Metode Imai-Matsumoto pada lapangan hingga GF(2^m)

Dimas Trisnadi, author

Abstrak

Metode dalam kriptografi dibedakan menjadi dua berdasarkan jenis kunci yang digunakan, yaitu metode simetris dan metode asimetris. Salah satu metode asimetris dalam kriptografi adalah metode Imai-Matsumoto. Dalam tugas akhir ini akan dibahas tentang cara kerja metode Imai-Matsumoto yang bekerja pada lapangan hingga 2 m GF . Metode ini menggunakan dua jenis kunci yang berbeda yaitu kunci pribadi dan kunci umum. Kunci umum pada metode ini dibentuk dari kunci pribadi yang dipilih oleh sipengguna metode.