IndoMS Journal on Industrial and Applied Mathematics
Volume. **1**, Issue. 1 (2014), pp. 21-26

DESAIN PERTUKARAN KUNCI MENGGUNAKAN INVERS KIRI (KANAN) MATRIKS

BUDI MURTIYASA*

Abstract. The research addresses to develop an application of theory of matrices, especially the left (right) inverses of matrices in the field of Z_2, on a key exchange scheme. A key exchange scheme development is based on Diffie-Hellman scheme. The result of research is that the key-exchange scheme is efficient enough in use of key space and is low complexity which is family of $O(n^2)$.

Key words. *left (right) inverses, key-exchange, cryptography*

Abstrak. Penelitian ini bertujuan mengembangkan penggunaan teori matriks, khususnya matriks invers kiri dan invers kanan dalam field Z_2, pada pembuatan skema pertukaran kunci. Skema dikembangkan berdasarkan model pertukaran kunci dari Diffie-Hellman. Berdasarkan skema pertukaran kunci yang telah dibuat, desain pembuatan kunci yang dipakai bersama cukup efisien dalam penggunaan ruang kunci serta mempunyai kompleksitas yang rendah, dalam hal ini anggota $O(n^2)$.

Kata kunci. *invers kiri (kanan), pertukaran kunci, kriptografi*