# MODIFICATION OF BLOCK CIPHER *IDEA*

Tomáš Majer

Department of Mathematical Methods, Faculty
of Management science and Informatics
University of Žilina
Veľký Diel, 010 26 Žilina, Slovak Republic
majer@frcatel.fri.utc.sk

The block cipher IDEA was presented in [2], its previous version PES was proposed in [1]. In both ciphers, the plaintext and the ciphertext are 64 bit blocks, while the secret key is 128 bits long.

IDEA were based on mixing operations from different algebraic groups. The required confusion was achieved by successively using three incompatible group operations on pairs of 16-bit subblocks.

This operations can not be easily expanded to 32-bit subblocks, because $2^{32}+1$ is not prime ($2^{16}+1$ is). It is possible to use multiplication modulo $2^{32}+1$, but not all elements have inverse element. This reduce number of usable keys and I study some cryptographic properties of this modification.

## References

[1] X.Lai, J.L.Massey: *A Propoposal for a New Block Encryption Standard*, Advances in Cryptology-EUROCRYPT'90, Springer-Verlag, 1991.

[2] X.Lai, J.L.Massey, S.Murphy: *Markov Ciphers and Differential Cryptanalysis*, Advances in Cryptology-EUROCRYPT'91, Springer-Verlag, 1991.