Abstract

As mathematical theory has evolved and computing capabilities have improved, what initially seemed to be adequately difficult trapdoor functions, were deemed not to be later. In this paper, a new block-encryption scheme named Modern Encryption Standard (MES) is proposed based on the multiple concepts arising from number theory for a highly secure and fast cryptosystem that can be considered as an alternative to the existing systems. This is a block cipher like AES, but the inherent algorithm is quite different. The security of the proposed MES algorithm stands on the fundamentals of the Chinese Remainder Theorem, Cantor Pairing Function and the Prime Number Theorem for creating an ingenious trapdoor function. Breaking this algorithm proves to be quite a daunting obstacle to overcome for an unwelcome interceptor.

References

doi:https://doi.org/10.1109/VLSISP.1995.527526
doi:https://doi.org/10.1007/s11432-010-4133-3
doi:https://doi.org/10.1007/BF02124750
doi:https://doi.org/10.1109/ACSAC.2000.898851
doi:https://doi.org/10.1017/S0305004100049252

Index Terms

Computer Science  Security
Keywords

AES, DES, NIST, MES, modern encryption, Modern Encryption Standard, 3DES, Triple DES, Chinese Remainder Theorem, Cantor Pairing Function, Shor's Algorithm, Pollard's Rho Algorithm