Symmetrix

Comparison of DES -AES



DES AES

Date 1976 1999

Block size 64 bits 128 bits

Key length 56 bits (effective 128, 192, 256 (and possibly more)

length) bits

Encryption primitives Substitution, Substitution, shift, bit mixing

permutation

Cryptographic Confusion, diffusion Confusion, diffusion

primitives

Design Open Open

Design rationale Closed Open

Selection process Secret Secret, but accepted open public

comment

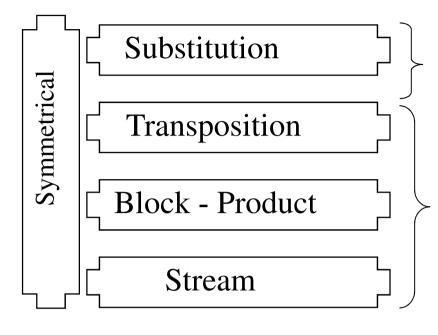
Source IBM, enhanced by Independent Dutch cryptographers

NSA

Assoc. Prof. Ahmet Koltukşuz, Ph.D.

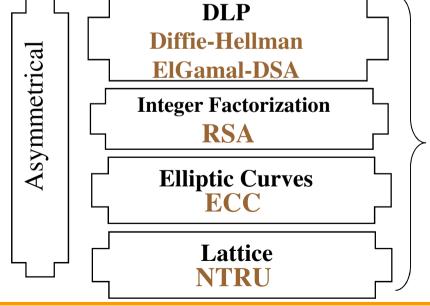
The Cryptographic Security





Security depends on the algorithm except one-time-pad.

Security depends on the KEY.



Security does not depend on the KEY.

Assoc. Prof. Ahmet Koltuksuz, Ph.D.