MT19937 stream cipher schema

key (PRNG seed)

Key stream
generator
(PRNG
MT19937)

stream i — 32 bits

32 to 8 bit
converter

stream i — 8 bits

Plaintext x_i 8 bits   8 bits   Ciphertext y_i

XOR