MT19937 stream cipher schema

key (PRNG seed)

key i   32 bits*

Key stream
generator
(PRNG
MT19937)

stream i   32 bits

32 to 8 bits
converter

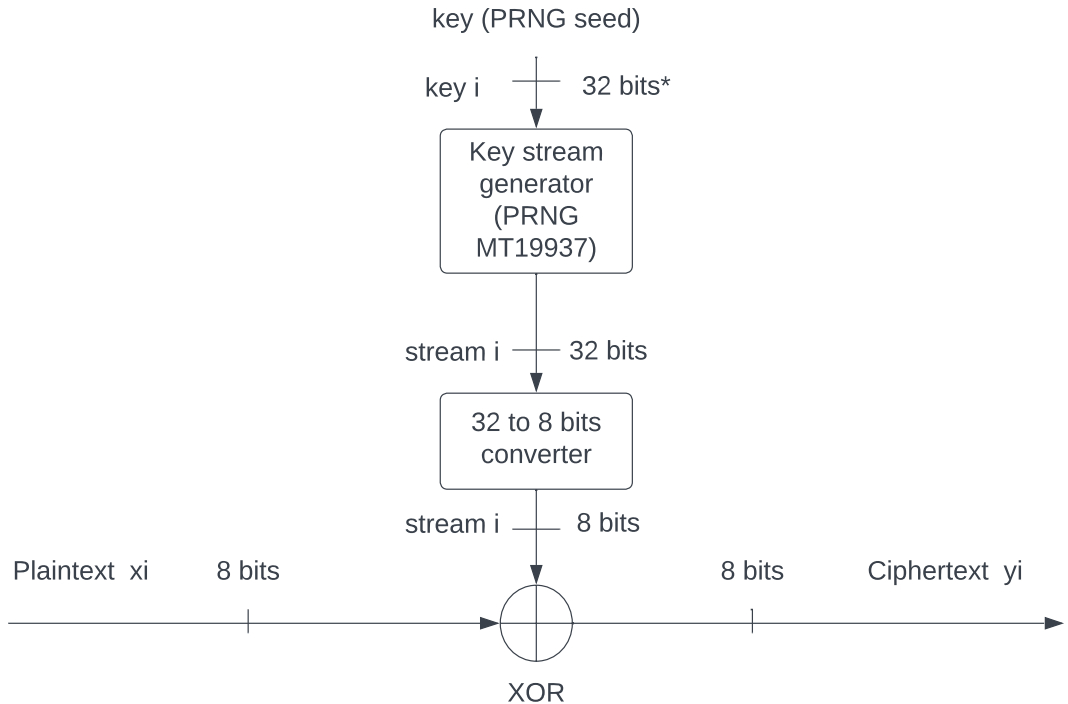stream i   8 bits

Plaintext x_i 8 bits   8 bits   Ciphertext y_i

XOR

- In this PRNG stream cipher, it was used 16-bit key size, to avoid waiting hours or a few days for a proof of concept of this kind of attack.