Decryption

enc_data

enc_Rand_key

Pri_key

Rand_key ← Block Crypto ← enc_Rand_key

Data ← stream cypher ← enc_Data