

4 Byte

4 Byte

Sequence
number

Ciphertext

random bytes

...

random bytes

DECRYPT

MAC

"Packet
length"

"Padding
length"

"Data"

...

"Padding"

"MAC"