

AES_ctx

+ RoundKey

+ Iv