



# 《白夜追凶》中的密码学原理



防火墙至少都是六十四位加密的

A close-up shot of a man with a mustache, wearing a dark jacket, shouting with his mouth wide open. His eyes are squeezed shut, and his facial muscles are tensed, conveying a sense of urgency or anger. The background is dark and out of focus.

你但凡涉及到安防监控



甚至可能是一百二十八位加密的

# 讨论台词的合理性

- 两句主要台词

- “防火墙至少是64位加密”
- “安防系统是128位加密”



- 如果使用以下类型加密体制，分别讨论两句台词合理性

- 对称密码（AES）
- 传统公钥加密（RSA等）
- ECC

## • 解答

- 第一句：不论使用哪种加密体制，64位都太短了，  
所以不合理
- 第二句：使用AES合理，AES密钥长度可以是128位  
使用RSA等传统公钥不合理，密钥长度太短  
使用ECC不合理，建议使用至少160位的ECC