密码学原语

安全漏洞可能导致灾难性后果。
因此，安全需求属于排除性需求。
然而，当系统遭受蓄意攻击时，安全漏洞才会暴露出来。

安全分析与保障工作包括识别关键资产、确定潜在漏洞及可能的攻击方式，并实施和测试安全解决方案。

与可靠性（随时间推移和使用次数增加而不断提升）不同，安全性的增长模型尚未得到充分确立。

假设A想要远程向B发送一条消息

可能存在哪些漏洞?

漏洞	解决方案
窃听	加密
伪装	身份验证与授权
消息篡改	消息摘要、消息认证码、数字签名
重播	时间戳与一次性随机数（Nonce）

密码学

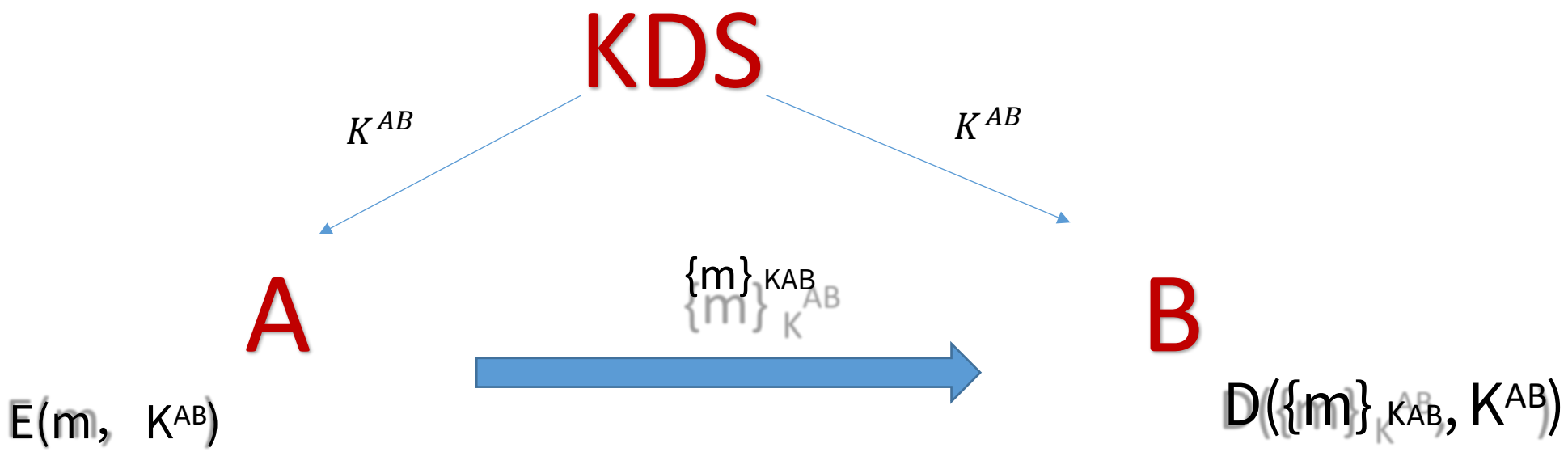
对称加密

- 流密码（例如 RC4）
- 分组密码（例如 AES、DES）

非对称加密

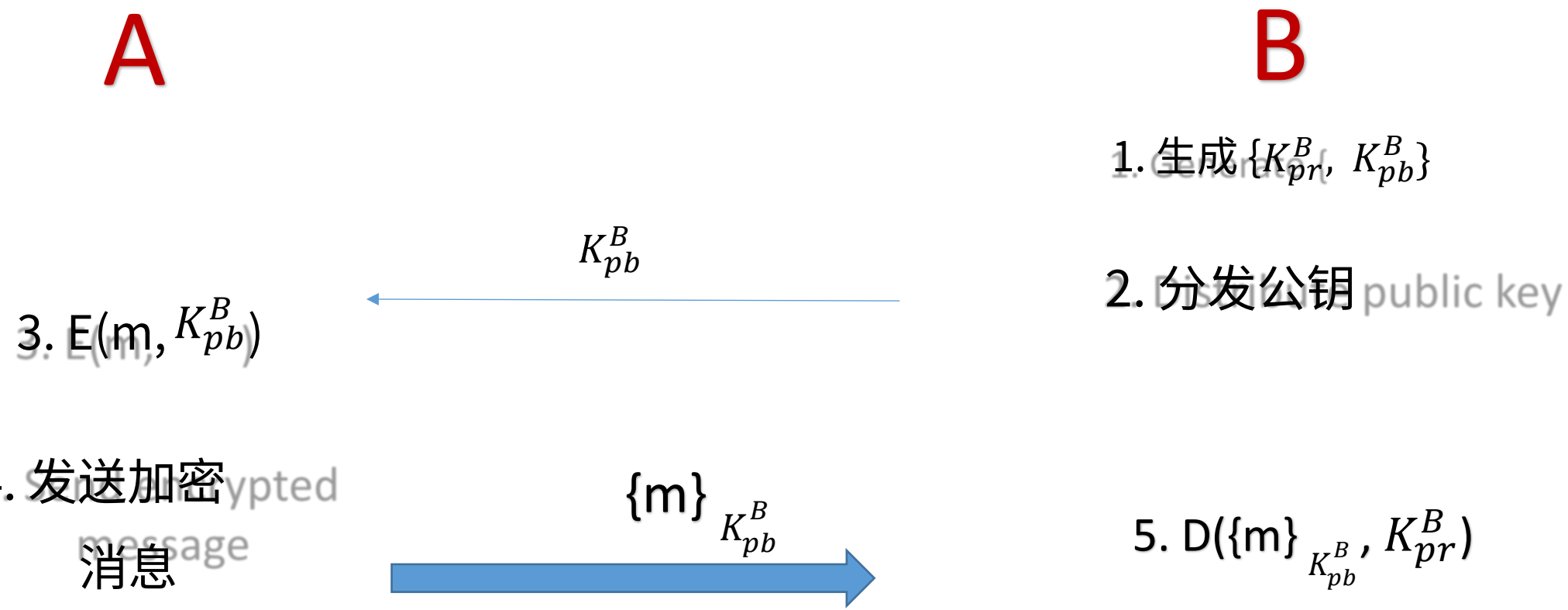
- RSA, Diffie-Hellman 和 ElGamal

对称密码学



- 加密和解密使用同一个共享密钥
- E 和 D 是公开已知的，而共享密钥是保密的
- 密钥分发信道必须既私密又真实
- 更快

非对称加密



- 公钥用于加密，私钥用于解密
- E、D 及公钥均为公开信息，而私钥则为机密信息
- 密钥分发信道必须具备真实性，以防止中间人攻击
- CPU 密集型

- 消息摘要，例如 MD5、SHA 消息摘要或哈希函数用于验证消息的完整性。

- 消息认证码，例如 HMAC-MD5、HMAC-SHA MAC（消息认证码）旨在使接收方确信该消息确实由发送方创建。

- 数字签名，例如 X509 证书

除了验证 ying 消息的grity 完整性和真实性y 类似于 MAC , a dig 意大利语 g 自然还提供不可否认性保护。消息发送方通过创建数字签名来实现这一点

即使用其私钥对消息摘要进行加密。若消息接收方能够利用签名者的经认证公钥成功恢复出消息摘要，则可确保不可否认性。

网络协议栈中的安全解决方案

应用层	**oAuth** **• 对应用程序进行认证以访问用户数据 反垃圾信息• 基于内容过滤消息**
运输	TLS/SSL • 保障隐私 • 身份验证（默认在服务器端执行，但也支持客户端验证）防火墙 • 根据端口号过滤数据包
网络	VPN（例如 IPSec、PPTP） • 保障隐私• 隧道端点的身份验证 防火墙 • 根据IP地址过滤数据包
	802.11x、WPA