Cryptographic Primitives

密码学原语

Security vulnerabilities could lead to catastrophic consequences.

Security requirements are thus excluding requirements.

Security vulnerabilities are however exposed when system is deliberately attacked

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。

Security analysis & assurance involves identifying valuable assets, determining vulnerabilities and possible attacks, applying and testing security solutions.

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，并应用和测试安全解决方案。

Unlike Reliability which improves as time goes by and usage increases, security growth models are not well established.

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

Suppose A wants to send a message to B remotely

What are the possible vulnerabilities ?

Vulnerabilities	Solutions
Eavesdropping	Encryption
Masquerading	Authentication & Authorization
Message Tempering	Message Digests, Message Authentication Codes, Digital Signatures
Replay	Timestamps and Nonce

假设 A 希望远程向 B 发送一条消息

可能存在哪些安全漏洞?

安全漏洞	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）

Cryptography

Symmetric

- Stream Ciphers e.g. RC4
- Block Ciphers e.g. AES, DES

Asymmetric

- RSA, Diffi-Hellman and ElGamal

密码学

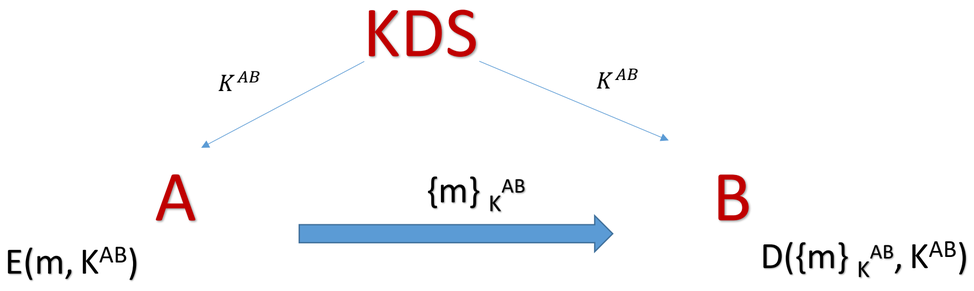
对称加密

- 流密码（例如 RC4）
- 分组密码（例如 AES、DES）

非对称加密

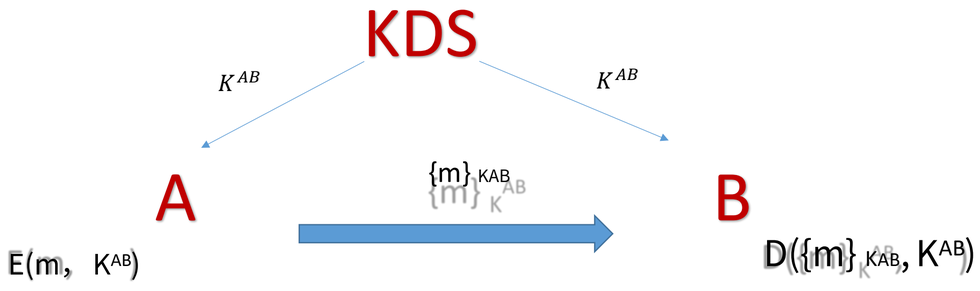
- RSA，Diffie-Hellman 和 ElGamal

Symmetric Cryptography



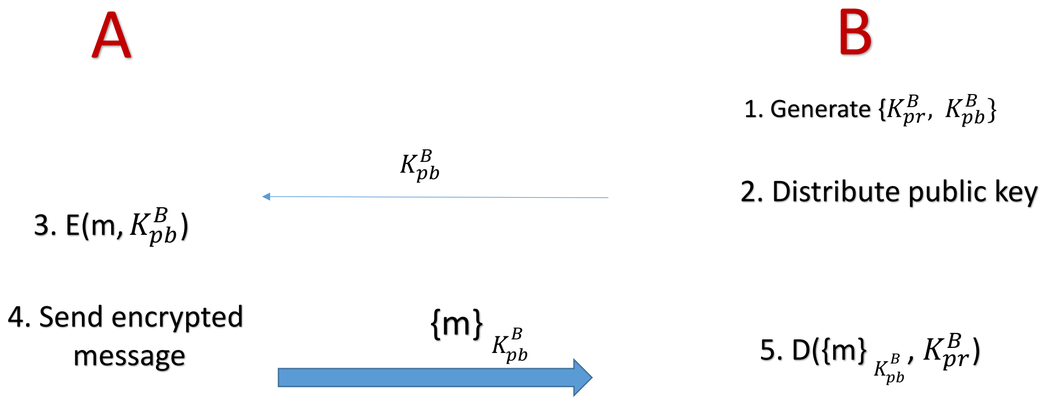
- A shared key is used for both encryption and decryption
- E and D are publically known whereas shared key is secret
- Key distribution channels need to be both private and authentic
- Faster

对称密码学



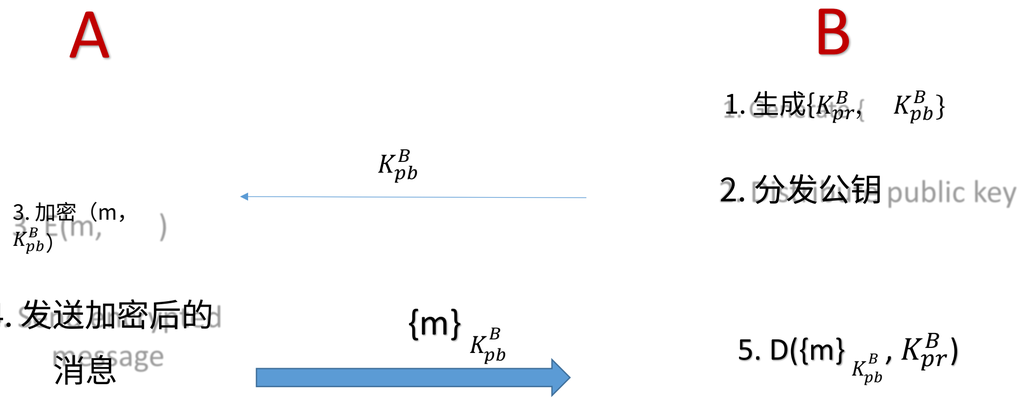
- 加密与解密使用同一共享密钥。
- E 和 D 是公开已知的，而共享密钥则为机密。
- 密钥分发信道必须同时具备私密性与真实性。
- 速度更快。

Asymmetric Cryptography



- Public key is used for encryption and private key for decryption
- E, D and the public key are known but private key is secret
- Key distribution channels need to be authentic to prevent man-in-the-middle attack
- cpu intensive

非对称加密



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

- **Message Digest e.g. MD5, SHA**
  Message digests or Hash functions are used to verify message integrity.

- **Message Authentication Codes e.g. HMAC-MD5, HMAC-SHA**

MAC (Message Authentication Code) is meant to establish the confidence in the recipient that the message was indeed created by the sender.

- **Digital Signatures e.g. X509 certificates**

In addition to verifying the integrity and authenticity like a MAC, a digital signature also protects non-repudiation. The sender of a message creates a digital signature by encrypting the message digest with his/her private key. Non-repudiation is thus guaranteed if the message recipient is able to recover the message digest using the certified public key of the signer.

- 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）消息认证码（MAC）旨在使接收方确信该消息确实由发送方生成。

- 数字签名（例如 X.509 证书）

数字签名除具备与消息认证码（MAC）相同的完整性与真实性验证功能外，还提供不可否认性保障。消息发送方使用其私钥对消息摘要进行加密，从而生成数字签名；若消息接收方能够利用签发者经认证的公钥成功恢复出该消息摘要，则可确保不可否认性。

Security Solutions in Network Stack

Application	**oAuth** • **Authenticates applications to consume user data** **Anti-Spam** • **Filters messages based on content**
Transport	TLS/SSL • Ensures Privacy • Authentication (by default server side but can also authenticate client side) Firewall • Filters packets based on port numbers
Network	VPN e.g. IPSec, PPTP • Ensures Privacy • Authentication of tunnel end points Firewall • Filters packets based on IP address
	802.11x, WPA

网络协议栈中的安全解决方案

应用层	OAuth • **对应用程序进行身份验证，以授权其访问用户数据；反垃圾邮件** • **基于消息内容进行过滤**
运输	TLS/SSL • 保障隐私性 • 身份认证（默认为服务器端认证，也可支持客户端认证）防火墙 • 基于端口号过滤数据包
网络	VPN（例如 IPSec、PPTP） • 保障隐私• 隧道端点身份认证 防火墙 • 根据IP地址过滤数据包
	802.11x ，WPA