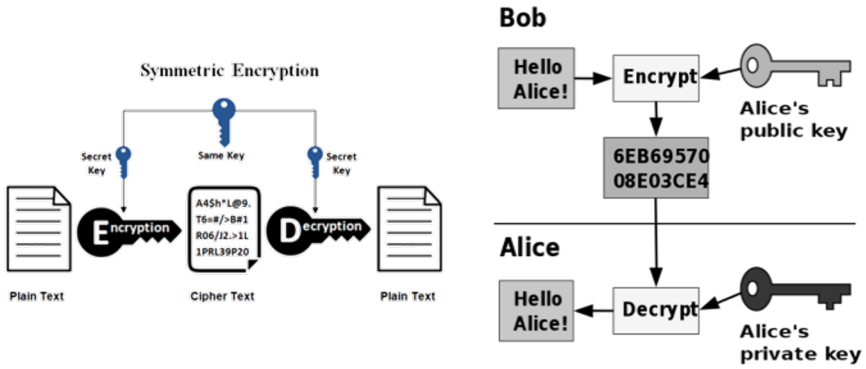
大纲

- 密码学应用分类
- 密码学在数据安全中的应用
- 密码学应用常见安全问题及案例
- 密码学应用实践建议

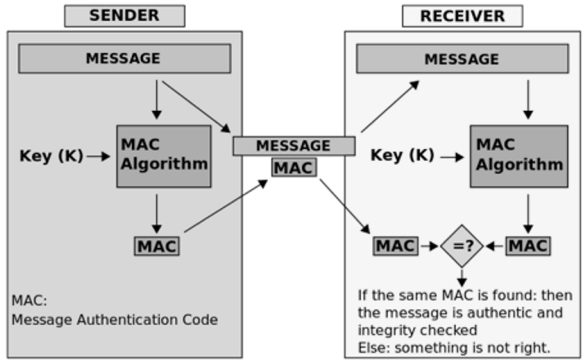
上个10年层出不穷的脱库和撞库悲剧告诉我们

「光靠存取控制（ACL）等手段来保护重要信息、数据是远远不够的」

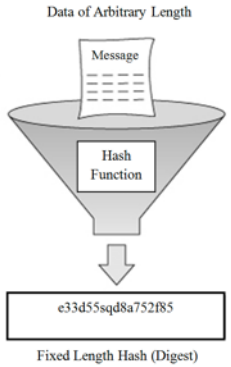
密码学应用分类



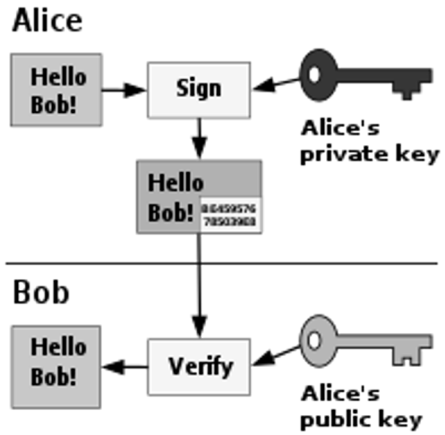
加解密（分组、流式）



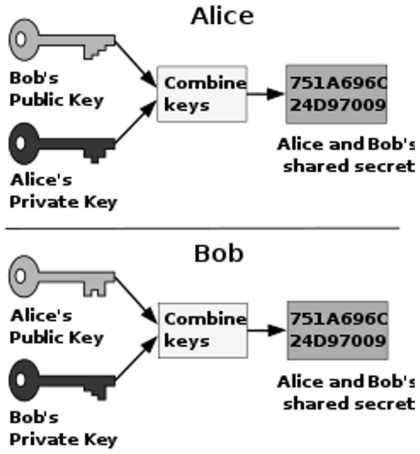
消息验证码



安全哈希



加验签



密钥交换

密码学的其他分类方式

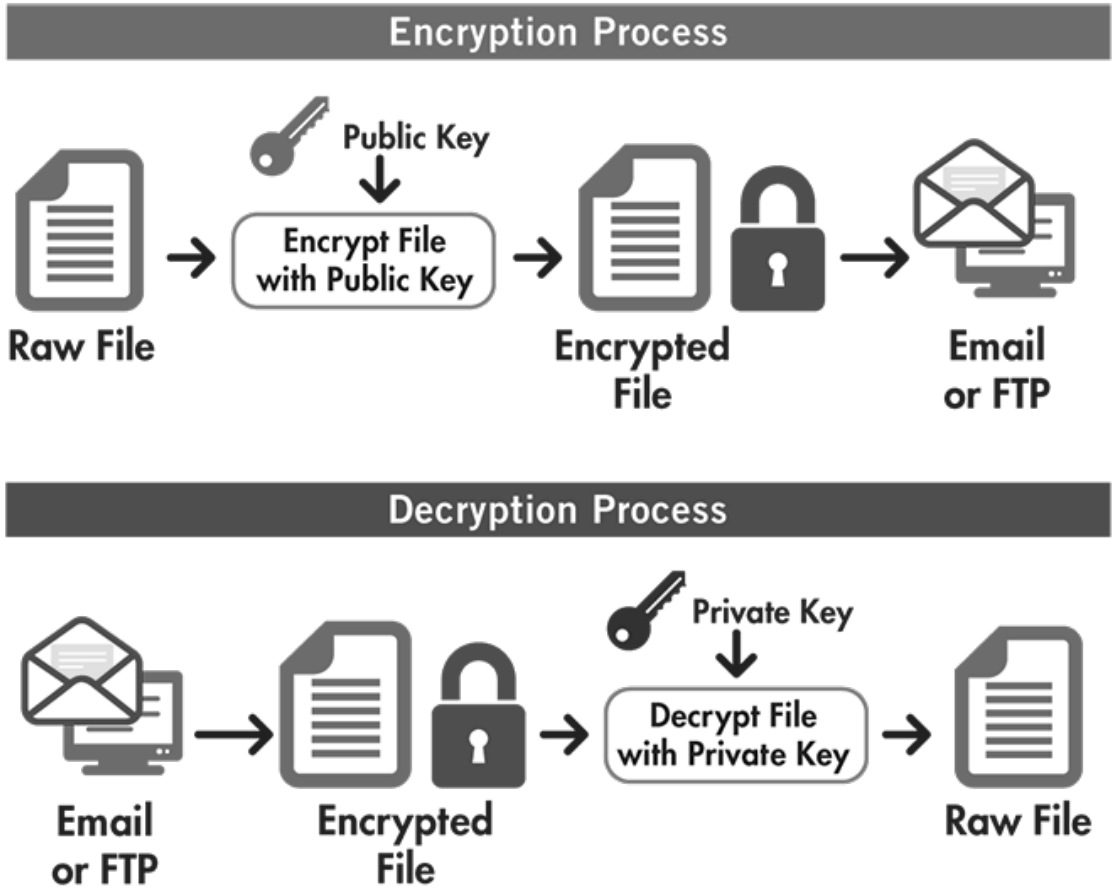
基于密钥体系	描述	常见算法
公钥（非对称）密码学	所使用密钥分为需要保密的私钥及可以公开的公钥。一部分密码学计算使用私钥来进行，一部分计算使用公钥来进行	RSA、ECDSA、X25519
对称密码学	密码学操作是用一个密钥来进行的	AES、HMAC

基于保密手段	描述	案例
算法密码学	通过对算法进行保密的方式来实现加密数据（密文）的保密性	各种自研加密实现
密钥密码学	公开算法，但密文的保密性是使用密钥来实现的	业界通用做法（柯克霍夫原则）

密码学在信息安全中的应用

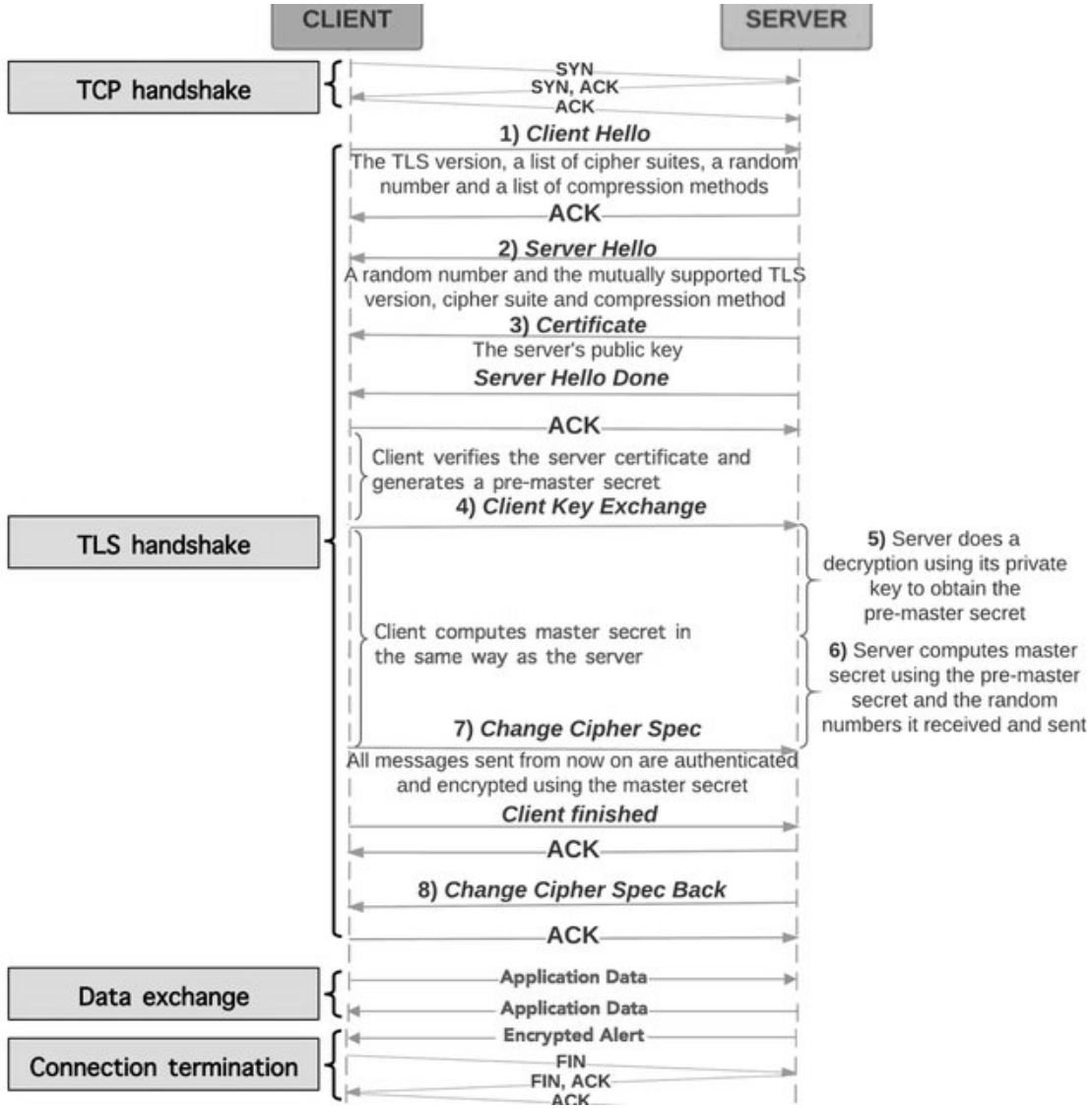
- 使用组合密码学手段以实现
  - 机密性 - Confidentiality
  - 完整性 - Integrity
  - 真实性 - Authenticity
  - 不可抵赖性 – Non-repudiation
- 密码学应用挑战随着时间变化不断演进
  - 硬件计算能力按照摩尔定律不断提升，软件架构水平也在不断提升
  - 密码学算法经常在分析、攻防中被证明有漏洞、有后门或可暴力攻破
- 公钥密码学一般不用于消息的直接加解密

密码学在信息安全中的应用案例-PGP



算法类型	算法
密钥协商	ElGamal (Diffie-Hellman)、ECDH
加验签-可验证性	DSA、ECDSA
分组加解密	3DES、AES-128、CAST-128、IDEA、Camellia
安全哈希	SHA-1

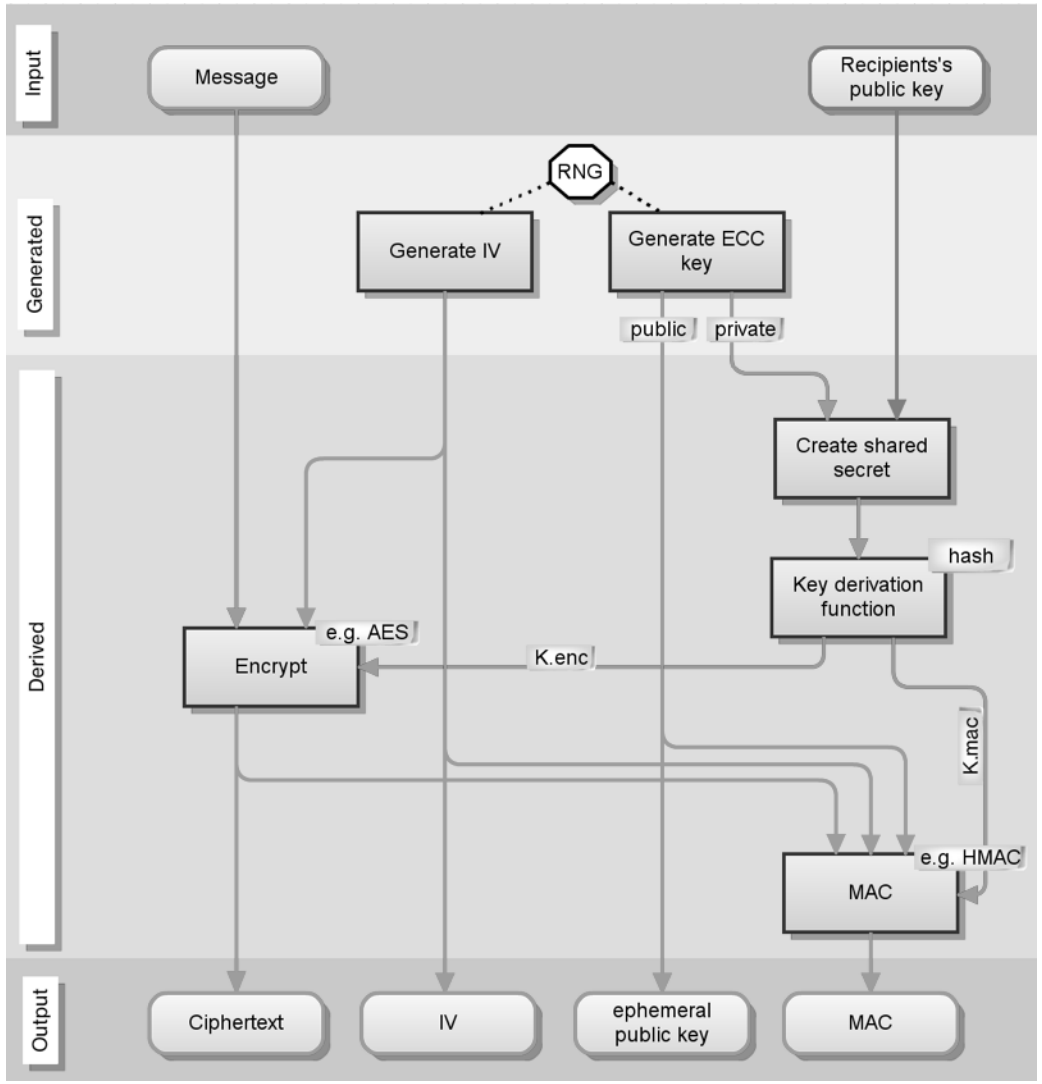
密码学在信息安全中的应用案例-HTTPS



算法类型	算法
密钥协商及可验证性	RSA、RSA-DH、DHE-RSA、DH-DSS、ECDH-ECDSA、ECDHE-EdDSA、PSK、PSK-RSA、SRP、SRP-DSS、SRP-RSA、Kerberos、DH-ANON、ECDH-ANON、GOST
分组加解密	AES (GCM、CCM、CBC)、Camellia (GCM、CBC)、ARIA (GCM, CBC)、SEED (CBC)、3DES-EDE (CBC)、GOST (CNT)、IDEA (CBC)、DES (CBC)、RC2 (CBC)
流式加解密	Chacha2-Poly1305、RC4

标准里有欧美日韩俄，没有中国

密码学在信息安全中的应用案例-ECIES



算法出现背景

1、ECC的安全等级在常见位长下是RSA的11倍+

2、ECC由于数学原理与ECC迥异，因此密钥对不能直接用于加解密

symmetric key	ECC	RSA
48	96	480
56	112	640
80	160	1248
112	224	2048
128	256	3248
256	512	15424

算法类型	算法
密钥生成	可自定义KDF
密钥协商	ECDHE
加验签-可验证性	MAC (e.g., HMAC-SHA-256)
分组加解密	e.g., AES、3DES(TDEA)

密码学应用常见安全问题

- 算法或实现本身存在或出现问题
  - ✗ 密码学算法已经被证明不安全
  - ✗ 密码学算法或实现中存在后门
  - ✗ 软硬件技术进步带来的算法被破解隐忧
- 算法使用不当而造成安全问题的
  - ✗ 没有保证盐(salt)、随机数(nonce)、临时密钥 (ephemeral key)、初始化向量(iv)等的随机性或临时性
  - ✗ 没有考虑密钥(secret key)的存储及使用的保密性需求，而造成密钥泄漏 – 如同公共保险箱的钥匙被人拿到
- 被别人用密码学分析手段进行了攻破
- 在明文、前像数据空间有限的场景下使用密码学

密码学应用常见安全问题 – 算法本身被发现存在问题

MD5和SHA-1加密算法被我国密码学家王小云破解

视频链接

如果说MD5和SHA-1是当今各种信息安全体系所依赖的大厦基石，那么现在，这些大厦的基础已经出现了很大的裂缝，甚至，有崩塌的危险。

全球学界震惊，美国军方网络在内的重大安全体系人人自危.....

2016年NSA建议的安全密钥长度

算法	使用场景
RSA 3072位以上	密钥交换、数字签名
Diffie-Hellman (DH) 3072位以上	密钥交换
ECDH with NIST P-384	密钥交换
ECDSA with NIST P-384	数字签名
SHA-384	完整性
AES-256	保密性

密码学应用常见安全问题 – 算法或者实现被埋了后门

In September 2013, *The New York Times* reported that internal NSA memos leaked by Edward Snowden indicated that the NSA had worked during the standardization process to eventually become the sole editor of the Dual_EC_DRBG standard,[7] and concluded that the Dual_EC_DRBG standard did indeed contain a backdoor for the NSA.[8] As response, NIST stated that "NIST would not deliberately weaken a cryptographic standard."[9] According to the *New York Times* story, the NSA spends $250 million per year to insert backdoors in software and hardware as part of the Bullrun program.[10] A Presidential advisory committee subsequently set up to examine NSA's conduct recommended among other things that the US government "fully support and not undermine efforts to create encryption standards".[11]
On April 21, 2014, NIST withdrew Dual_EC_DRBG from its draft guidance on random number generators recommending "current users of Dual_EC_DRBG transition to one of the three remaining approved algorithms as quickly as possible."

密码学应用常见安全问题 – 用常量代替随机数或随机数可预测

PS3

PlayStation 3

GAMING & CULTURE —

PS3 hacked through poor cryptography implementation

A group of hackers named fail0verflow revealed in a presentation how they ...

CASEY JOHNSTON - 12/31/2010, 1:25 AM

158

A group of hackers called fail0verflow claim they've figured out a way to get better control over a PlayStation 3 than ever before. After they worked through a number of Sony's security measures, they found the keystone to gaining access to the system's innards was the PS3's poor use of public key cryptography.

At the Chaos Communication Conference 27C3, the team gave a 45-minute presentation on the methods they used to work through the PS3's various security levels, which include a chain of trust, a hypervisor, and signed executables. Their primary goal was to restore the capability to run Linux, something that was forcibly removed from the original PS3 and never possible on the PS3 Slim.

After beating several other security measures, the group was able to locate the PS3's ECDSA signature, a private cryptographic key needed to sign off on high-level operations. Normally, these kinds of keys are difficult to figure out, and require running many generations of keys to crack.

But when fail0verflow worked backwards from generated keys, they found out that a parameter that should have been randomized for each key generation wasn't being randomized at all. Instead, the PS3 was using the same number for that variable, every single time, making it easy to work out acceptable keys.

If this really works, it's a big slip on Sony's part. While PS3s are no stranger to software updates, this seems like it might affect operation on too many levels to be an easy fix. Fail0verflow's presentation is available in three parts on YouTube, and they also plan to put up a demo of their methods on their website.

密码学应用常见安全问题 – 密码学分析+传统网络、软件攻击

暴力攻击（字典攻击）	回旋镖攻击
重放攻击	戴维斯攻击
中间人攻击	长度延伸攻击
碰撞攻击	差值密码学分析
前像攻击	XSL攻击
降级攻击	模-n密码学分析
已知明文攻击	线性密码学分析
挑选明文攻击	整数部密码学分析
相关密钥攻击	滑动攻击
生日攻击	三明治攻击
彩虹表攻击	中间相会攻击
黑袋密码学分析	窃听攻击
功耗分析	…
耗时分析	…

密码学应用常见安全问题 – 思考题

因为安全哈希在设计上满足确定性、不可碰撞碰撞性及前像不可逆推等性质：

$\because \forall A \neq B, Hash(A) \neq Hash(B)$

$\therefore \exists Hash(A) = Hash(B) \Rightarrow A = B$

所以很多人喜欢用安全哈希匹配来取代ID匹配，认为这个既保护了ID前像，还能达到业务目的。譬如说两家公司在进行业务撞库时，以手机号为ID。

但是这个应用设计存在着巨大的安全隐患，大家想一下是为什么？

密码学实现信息安全实践建议

- 不要自己造算法轮子（但可以组合现有算法）
- 不要用已经暴雷的算法，采用足够安全的密钥长度
- 密钥创建时一定要保证有足够的随机性及墒值
- 算法中建议随机数、临时密钥等一定要保证其随机性及临时性
- 不要在不安全的环境下存储、使用密钥，保证密钥使用场景的安全性
- 要考虑计算技术的进步带来的影响，譬如说量子计算机
- 综合使用多种密码学手段，乃至非密码学手段来实现应用设计
- 应用算法设计上要留有版本及升级能力（隐含：向后兼容）
- 追踪最新的安全攻击方式及密码学成果，及时加固升级
- 数据机密哪怕是密文、承诺等都尽量避免第三方持久化获得
- 数据机密保护要考虑对抗侧信道攻击、社会工程学攻击等方式
- 用对抗思路、乃至引入蓝军做法来设计密码学应用，不要闭门造车
- 在有条件的情况下，考虑使用国密来实现合规条件下的保密