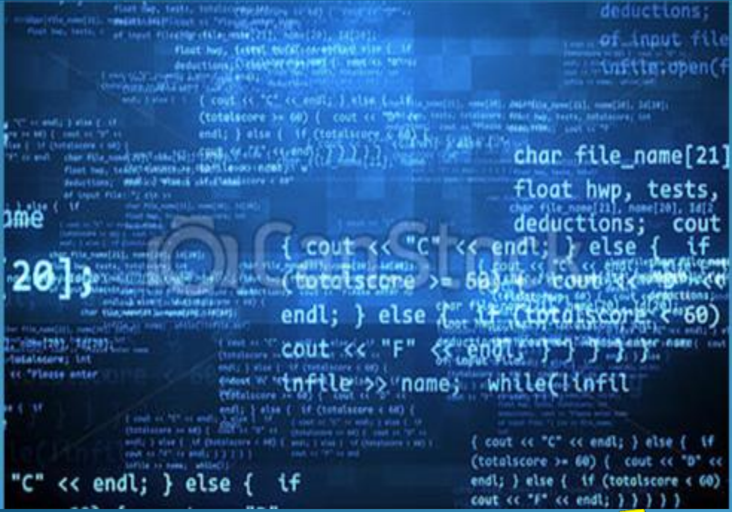

密码学理论与应用

数据完整性保护

消息认证、数字签名

$$ed = 1 \bmod \varphi(N)$$

$$Y = M^e \bmod N$$

$$M = Y^d \bmod N$$

数据完整性保护方案

- 基本概念
- 消息认证方案和数字签名方案都属于构造各类计算机密码方案和协议的最基本的工具，其安全性在本质上都是某种意义上的抗伪造性质。
- 消息认证方案(*message authentication*)：对称机制
- 数字签名方案(*digital signature*)：非对称机制

消息认证方案(1)

- MAC Scheme：工作方式和安全目标
-
- 一、消息认证方案(*Message Authentication*)用于保证数据一致性，防止数据在从发送方到达接收方的过程中被篡改。
- 为达到防篡改的目的，发送方和接收方事先获得一个共享密钥K，发送方以该密钥为参数计算数据认证码$\sigma \leftarrow MAC(K,M)$, 发送$(M, \sigma)$;
- 接收方则以该密钥K为参数对数据M和认证码σ进行验证：$Vf(K, M, \sigma) \stackrel{?}{=} 1$.
- 二、 消息认证方案的安全目标在于：任何攻击者在未知密钥的情况下，不可能有效伪造出正确的消息认证码σ。

消息认证方案(2)

- MAC方案的简单实现：

- 借助于一个对称加密方案(KG, E, D)，MAC方案可构造如下：
- 对称密钥K：$K \leftarrow KG(k)$；
- 消息认证码生成算法MAC(K,M):
- $\sigma \leftarrow E(K, M)$;
- 消息认证码认证算法Vf(K,M, σ):
- $M \overset{?}{=} D(K, \sigma)$;
- 注1 如果对称加密方案CCA-安全，则上述MAC方案抗伪造。
- 注2 上述构造并非最具计算效率的方法，达成相同安全目的
- 同时在效率上更为实用的方法，参阅Stallings教程11.5和12.5
- (或因特网标准RFC)。

消息认证方案(3)

- **消息认证方案安全模型: (KG,MAC,Vf)的抗伪造性**

P： 认证密钥持有者　　k是安全参数　　A：伪造者/P.P.T算法

1. $K \leftarrow \mathrm{KG}(k)$

2. $|K|$ (P → A)

3. $(St, \{M_k\}_{k=1,\ldots,N}) \leftarrow \mathrm{A1}(|K|)$

4. $\{M_k\}_{k=1,\ldots,N}$ (A → P)

5. $\sigma_k \leftarrow MAC(K, M_k)$;

6. $\{\sigma_k\}_{k=1,\ldots,N}$ (P → A)

7. $(M^*, \sigma^*) \leftarrow \mathrm{A}_2(St, \{\sigma_k\}_{k=1,\ldots,N})$: $\mathrm{M}^* \neq \mathrm{M}_k$

8. M^*, σ^* (A → P)

9. $Vf(K, M^*, \sigma^*) \stackrel{?}{=} 1$;

- 消息认证方案定义做**CMF-不安全**(*in-Secure Against Chosen Message Forge*)，若存在*P.P.T.*算法A和多项式$poly_0(k)$，对$k \to \infty$满足
- $$P[Vf(K, M^*, \sigma^*) = 1] \geq 1/\mathrm{poly}_0(k)$$

【思考】MAC方案抗伪造、但不抗抵赖，为什么？　注意同数字签名方案在这方面的区别！

数字签名方案(1)

- 关于安全散列函数(*Security Hash*)的预备知识

- 1\. 一个字符串到字符串的映射***H***：$\{0,1\}^+ \rightarrow \{0,1\}^k$相伴随的三类问题：
- (已知条件：*H*的算法逻辑，且存在高效算法从*x*计算*H*(*x*))
  - 第一类原像问题：对任何***y***，求任何满足***y***=H(***x***)的*x*；
  - 第二类原像问题：对任何***y***和***x***，求任何满足***y***=H(***x****)的$x^* \neq x$；
  - 冲突问题：求$x^* \neq x$使$H(\boldsymbol{x}^*)=H(\boldsymbol{x})$。

2\. ***H***的安全性质：

H定义做抗第一类原像攻击，若第一类原像问题难解；

H定义做抗第二类原像攻击，若第二类原像问题难解；

H定义做抗冲突(collision-free)，若其冲突问题难解；

3\. 具有以上性质的***H***的实例：基于MD-5或SHA的*HMAC*等标准算法。

数字签名方案(2) Stallings教程：13.1~13.4

- 数字签名方案(*Digital Signature*)：基本概念

- 1. 数字签名方案Ξ = (KG, Sig, Vf)是一组算法*KG*、*Sig*和*Vf*。
- 设k是复杂度参数，*KG* 是密钥生成算法，输出公钥/私钥对(pk,sk)，其中公钥pk被公开，私钥sk则仅被签名者持有。
- *Sig*是签名算法，以私钥sk和消息M为输入，计算签名$\sigma=\mathrm{Sig}(sk,M)$。
- *Vf*是验证算法，以公钥pk、消息M和字串σ为输入并输出验证结果，
- 1表示接受(验证成功)、0表示拒绝(验证失败)：$Vf(pk,M,\sigma) \overset{?}{=} 1$。

- 2. KG, Sig 和Vf须满足一致性关系：对任何k 和M恒有
- $P[(pk,sk)\leftarrow \mathrm{KG}(k); \sigma\leftarrow \mathrm{Sig}(sk, \mathrm{M}): \mathrm{Vf}(pk,M, \sigma)=1]=1$

数字签名方案(3)

Stallings教程：13.1~13.4

- **数字签名方案安全模型: (KG,Sig,Vf)的抗伪造性**

P： 签名私钥持有者　　***k***是安全参数　　A：伪造者/P.P.T算法

1. $(pk, sk) \leftarrow \mathrm{KG}(k)$
2. pk (P → A)
3. $(St,\{M_k\}_{k=1,\dots,N}) \leftarrow \mathrm{A1}(pk)$
4. $\{M_k\}_{k=1,\dots,N}$ (A → P)
5. $\sigma_k \leftarrow Sig(sk, M_k)$;
6. $\{\sigma_k\}_{k=1,\dots,N}$ (P → A)
7. $(M^*,\sigma^*) \leftarrow \mathrm{A}_2(St,\{\sigma_k\}_{k=1,\dots,N})$: $M^* \neq M_k$
8. M^*,σ^* (A → P)
9. $Vf(pk, M^*,\sigma^*) =^{?} 1$;

- 数字签名方案定义做**CMF-不安全**(*in-Secure Against Chosen Message Forge*)，若存在*P.P.T.*算法A和多项式$poly_0(k)$，对$k\rightarrow\infty$满足
- $$P[Vf(pk, M^*,\sigma^*) = 1] \geq 1/\mathrm{poly}_0(k)$$

【思考】数字签名方案抗伪造且抗抵赖，为什么？　注意同MAC方案在这方面的区别！

数字签名方案(4)

Stallings教程：13.1~13.4

- *ElGamal*签名方案(1985)

- 参数：p是所谓k位α-难解型素
- 示p的位数)，g是F_p^*的生成子，
- p、g、H是公开的参数。

- 公钥/私钥生成算法KG(k, g, p):
- $\boldsymbol{x} \leftarrow^{\$} \{1,2,\ldots,p\text{-}1\}$; $\boldsymbol{y} \leftarrow g^x \bmod p$

- 签名算法$Sig^H(x, M)$:
- $\boldsymbol{K} \leftarrow^{\$} F_p^*$; $\boldsymbol{r} \leftarrow g^K \bmod p$; $\boldsymbol{h} \leftarrow$
- $\sigma \leftarrow (r, h, s)$;
- 验证算法$Vf^H(y, M, (r,h,s))$:
- $\boldsymbol{h} = H(M \| r) \wedge g^h = y^r r^s \bmod p$;

安全性：

(因为F_p^*上的判定性Diffie-Hellman问题难解)，ElGamal方案具有CMF-抗伪造性。

证明：参阅Pointcheval & Stern，Security Proofs for Signature Schemes，Lecture Notes in Computer Sci., Vol. 1070.，1996.

其他实现：

ElGamal签名方案也可以在椭圆曲线上实现，并具有相同的抗伪造性（感兴趣的同学可参考教程13.5）。

一致性：

$y^r r^s = g^{xr} g^{Ks} = g^{Ks+xr} = g^{(Ks+xr) \bmod (p-1)} = g^h \bmod p$ （这里用到*Fermat*公式）

教材阅读：

消息认证码方案：11.2~11.3、11.5、12.1、12.5，以概念性的理解为主

数字签名方案：13.1~13.4，注意方案的细节与分析。