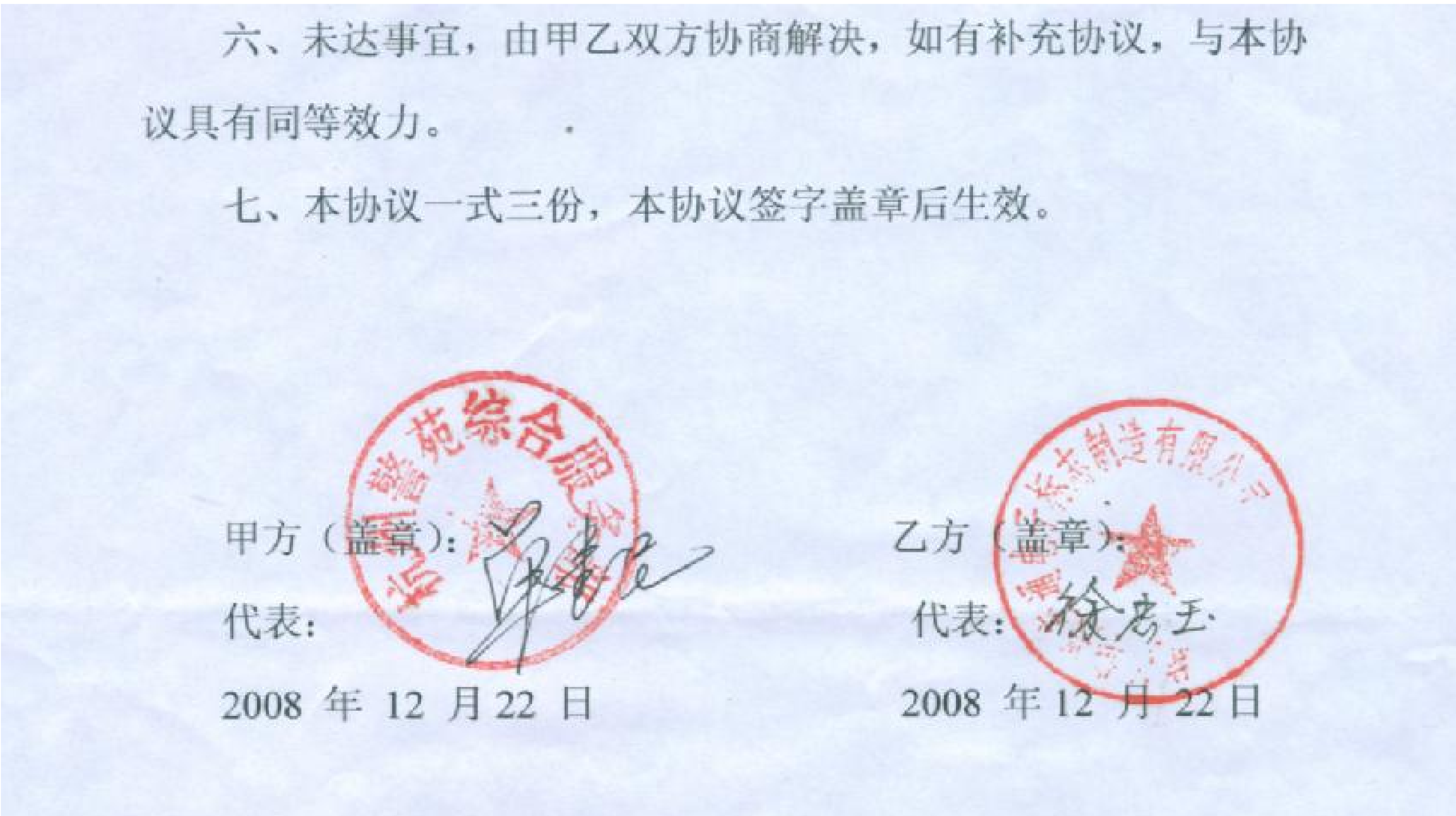
数字签名
Digital Signature

数字签名



六、未达事宜，由甲乙双方协商解决，如有补充协议，与本协议具有同等效力。

七、本协议一式三份，本协议签字盖章后生效。

甲方（盖章）：

代表：

2008 年 12 月 22 日

乙方（盖章）：

代表：

2008 年 12 月 22 日

数字签名算法

数字签名算法包括三个子算法：

1. 密钥生成子算法(Gen)
   算法输入：安全参数n；算法输出：签名密钥sk，验证密钥pk

2. 数字签名子算法(Sig)
   算法输入：签名密钥k和消息m；
   算法输出：签名s，s $\leftarrow$ Sig(sk, m)

3. 验证子算法(Vrfy)
   算法输入：验证密钥pk，消息m，签名s；
   算法输出：b=Vrfy(pk, m, s) 验证通过为1，验证失败为0

Vrfy(pk, m, Sig(sk, m)) = 1

数字签名介绍

签名方案的攻击模型

1）唯密钥攻击（key-only attack）

2）已知消息攻击（Known Message Attack）

3）选择消息攻击（Chosen Message Attack）

攻击者的目标

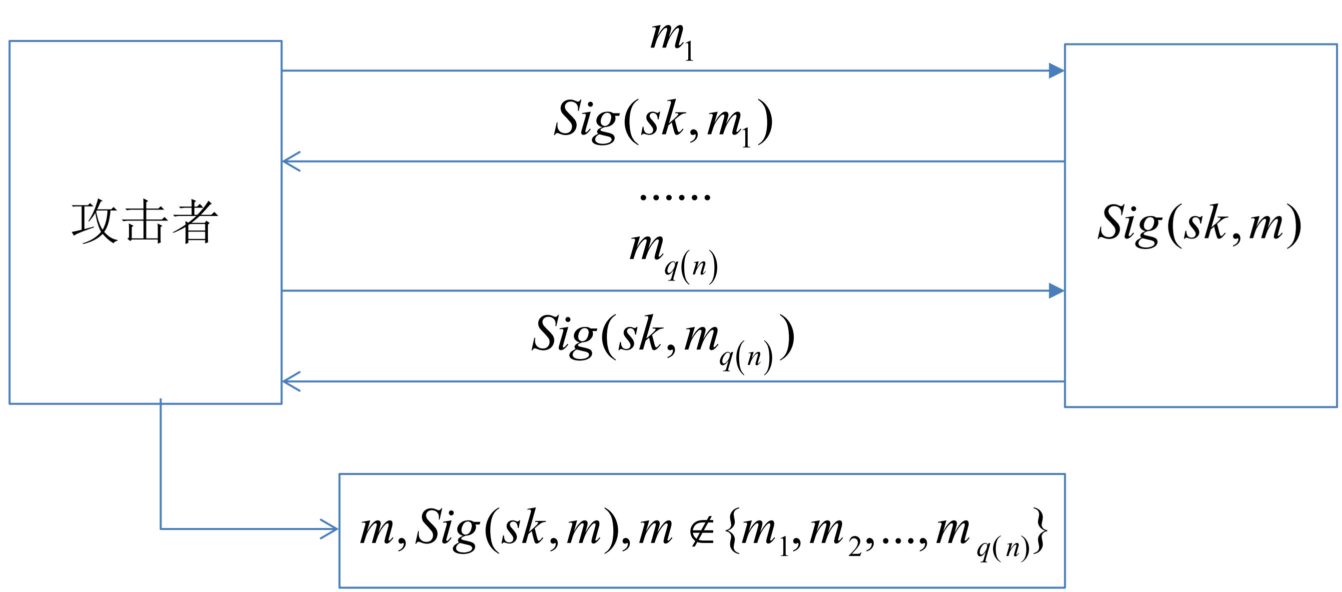
1）选择性伪造（Selective Forgery)

2）存在性伪造（Existential Forgery）

数字签名攻击实验

抵抗选择消息攻击的数字签名算法（Sig-forge 实验流程）

攻击者通过查询获得一些消息的签名，不能构造出没有查询过的消息的签名。



$$\Pr\left[\text{Sig-forge}_{\mathcal{A},\Pi}(n) = 1\right] \leq negl(n)$$

RSA签名方案

RSA签名：

$$\mathcal{K}=\{(n,p,q,a,b): n=pq, p\text{和}q\text{是素数，} \quad ab\equiv 1 \bmod (\phi(n))\}$$

(n,b)为公钥，(p,q,a)为私钥

对于$K=(n,p,q,a,b)$,定义

$$\text{sig}_K(x)=x^a \bmod n$$

$$\text{ver}_K(x,y)=\text{true} \Leftrightarrow x=y^b \bmod n$$

RSA签名方案

伪造签名：

1）选择$y \leftarrow Z_n$并计算$x = e_K(y) = y^e$，则y是x的有效签名。

2）已知合法消息签名对$(x_1, y_1), (x_2, y_2)$，可以构造消息 x_1x_2的签名为 y_1y_2。

3）已知x，计算$x \equiv x_1x_2 \bmod n$，分别请求计算x_1和x_2的签名 y_1和y_2，则x的签名为y_1y_2。

RSA签名方案

签名和HASH函数

消息	x	$x \in \{0, 1\}^*$
摘要	$z = Hash(x)$	$z \in Z$
签名	$y = sig(sk, x)$	$y \in \mathcal{A}$

$$ver_K(Hash(x), y) = 1$$

ElGamal签名方案

1985年提出了El Gamal签名方案。

El Gamal签名方案是非确定性的，也就是说对任意给定的消息有很多有效的签名。

El Gamal签名方案

El Gamal签名方案

设$\alpha \in Z_p$是一个生成元，$\mathcal{P}=Z_p^*, \mathcal{A}=Z_p^* \times Z_{p-1}$,定义

$$\mathcal{K}=\{(p,\alpha,b,\beta):\beta=\alpha^b\}$$

则p,α,β是公钥，b是私钥。

对$K=(p,\alpha,b,\beta)$和一个秘密随机数$r \in Z_{p-1}^*$,定义

$$sig_k(x,r)=(\gamma,\delta)$$

其中

$$\gamma=\alpha^r \bmod p, \delta=(x-b\gamma)r^{-1} \bmod (p-1)$$

对$x, \gamma \in Z_p^*$和$\delta \in Z_{p-1}$，定义

$$ver_K(x,(\gamma,\delta))=\text{true} \Leftrightarrow \beta^\gamma \gamma^\delta = \alpha^x \bmod p$$

El Gamal签名方案

例：$p=23,\alpha=5,b=6,\beta=5^6 \bmod 23=8$,求消息$x=10$签名。

随机选择k=7, 计算

$$\gamma=\alpha^k \bmod 23=5^7 \bmod 23=17 \bmod 23$$

$$\delta=(x-b\gamma)k^{-1} \bmod 22=(10-6*17)*19=12 \bmod 22$$

签名是$(17,12)$

验证：$\beta^\gamma\gamma^\delta=8^{17}17^{12}=9 \bmod 23$

$$\alpha^x=5^{10}=9 \bmod 23$$

El Gamal签名方案

例：$p=23, \alpha=5, b=6, \beta=5^6 \bmod 23=8$,求消息 $x=10$签名。

随机选择$r=5$, 计算

$$\gamma=\alpha^r \bmod 23=5^5 \bmod 23=20$$

$$\delta=(x-b\gamma)r^{-1} \bmod 22=(10-6*20)*9=0$$

签名是$(20,0)$

验证：$\beta^\gamma \gamma^\delta=8^{20}=9 \bmod 23$

$$\alpha^x=5^{10}=9 \bmod 23$$

El Gamal签名方案

如果泄露r，且$\gcd(\gamma, p-1)=1$，则可以很容易求出私钥b

$$\beta^{\gamma}\gamma^{\delta} \equiv \alpha^{b\gamma}\alpha^{r\delta} \equiv \alpha^{x} \bmod p$$

$$\Rightarrow b = (x - r\delta)\gamma^{-1} \bmod (p-1)$$

Schnorr签名方案

Schnorr签名方案

设q是能被$p-1$整除的素数，$\alpha \in Z_p^*$是1模p的q次根，

$h:\{0,1\}^* \to Z_q$是一个安全的hash函数。定义

$$\mathcal{K} = \{(p,q,\alpha,a,\beta) : \beta \equiv \alpha^a \pmod p, a \in Z_q\}$$

则p,q,α,β是公钥，a是私钥。

Schnorr签名方案

对$K=(p,q,\alpha,a,\beta)$和一个秘密随机数$r\in Z_q^*$,定义

$$sig_K(x,r)=(\gamma,\delta)$$

其中

$$\gamma=h(x\,\|\,\alpha^r \bmod p),\delta=r+a\gamma(\bmod q)。$$

对$x\in\{0,1\}^*,\gamma,\delta\in Z_q$,定义

$$ver_K(x,(\gamma,\delta))=\text{true}\Leftrightarrow h(x\,\|\,\alpha^\delta\beta^{-\gamma} \bmod p)=\gamma$$

数字签名算法(DSA)

数字签名算法(DSA)

设q是能被$p-1$整除的素数， $\alpha \in Z_p^*$是1模p的q次根，

定义

$$\mathcal{K} = \{(p, q, \alpha, b, \beta) : \beta \equiv \alpha^b \pmod p), b \in Z_q\}$$

则p, q, α, β是公钥， b是私钥。

数字签名算法(DSA)

对$K=(p,q,\alpha,b,\beta)$和一个秘密随机数$r\in Z_q^*$,定义

$$sig_k(x,r)=(\gamma,\delta)$$

其中

$$\gamma=(\alpha^r \bmod p)\bmod q$$

$$\delta=(\text{SHA-1}(x)+b\gamma)r^{-1} \bmod q$$

对$x\in\{0,1\}^*,\ \gamma,\delta\in Z_q$,定义

$$e_1=\text{SHA-1}(x)\delta^{-1}\bmod q$$

$$e_2=\gamma\delta^{-1}\bmod q$$

$$ver_K(x,(\gamma,\delta))=\text{true}\Leftrightarrow(\alpha^{e_1}\beta^{e_2}\bmod p)\bmod q=\gamma$$

椭圆曲线数字签名算法（ECDSA)

椭圆曲线数字签名算法(ECDSA)

设p是一个大素数，E是定义在F_p上的椭圆曲线。设A是E上阶为q的一个点，使得$\langle \mathrm{A} \rangle$上的离散对数问题是个困难问题。定义

$$\mathcal{K} = \{(p, q, E, A, m, B) : B \equiv mA, m \in Z_q\}$$

则p, q, E, A, B是公钥，m是私钥。

椭圆曲线数字签名算法（ECDSA)

对$K=(p,q,E,A,m,B)$和一个秘密随机数$k\in Z_q^*$,定义

$$sig_K(x,k)=(r,s)$$

其中

$$kA=(u,v)$$

$$r=u \bmod q$$

$$s=(\text{SHA-1}(x)+mr)k^{-1} \bmod q$$

椭圆曲线数字签名算法（ECDSA)

对$x \in \{0,1\}^*$, $r, s \in Z_q^*$, 验证过程如下

$$w = s^{-1} \bmod q$$

$$i = w\text{SHA-1}(x) \bmod q$$

$$j = wr \bmod q$$

$$(u, v) = iA + jB$$

$$ver_K(x, (r, s)) = \text{true} \Leftrightarrow u \bmod q = r$$

椭圆曲线数字签名算法（ECDSA)

例：定义在Z_{11}上的椭圆曲线$y^2=x^3+x+6$。签名方案的参数$p=11, q=13, A=(2,7), m=7, B=(7,2)$。假设消息$x$的哈希值为4,随机数$k$=3。计算签名并进行验证。