密码学理论与应用

数据完整性保护

消息认证、数字签名（习题）

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

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

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

关于散列函数与数字签名方案的习题

- 习题1　考虑以下散列函数H的设计方案
- (1) $H(x) = (x^2 + Ax + B) \bmod 2^m$：$\{0,1\}^m \rightarrow \{0,1\}^m$，$x$是任何$m$位的0-1串，将其
- 　　看做一个m位二进制整数; A和B是给定的m位二进制整数。
- (2) $H(x)$同上，但是作为 $\{0,1\}^n \rightarrow \{0,1\}^m$的散列函数，$n \geq m+1$, x是任何n位的0-1串，
- (3) $H(x) = (A_d x^d + A_{d-1} x^{d-1} + \ldots + A_1 x + A_0) \bmod 2^m$：$\{0,1\}^n \rightarrow \{0,1\}^m$，$n \geq m+1$, x是任何
- 　　n位的0-1串; A_j均为给定的m位二进制整数。
- 　　证明存在多项式复杂度算法$\mathscr{A}$，从x计算出$y(\neq x)$使得$H(x)=H(y)$.
- 　　因此，以上设计方案都不能抵抗第二类原像攻击（因此也不抗冲突）。
- 求解概要
- (1) 若$x \neq y \bmod 2^m$但$H(x)=H(y)$，则 $(x^2 + Ax + B) = (y^2 + Ay + B) \bmod 2^m$,
- 　　等价地 $x^2 - y^2 = Ay - Ax \bmod 2^m$, 于是 $x+y = -A \bmod 2^m$ 。
- 　　　　从上面这段粗略的分析，能得到什么启发？由此你能推断出如何
- 　　构造算法$\mathscr{A}$吗？写出该算法的公式，并验证之。
- (2) 这时存在更简洁的第二类原像攻击算法【提示：注意$n>m$】。
- 　　请思考：该算法对情形(1)是否还有效？
- (3) 推广情形(2)中的攻击算法。

关于散列函数与数字签名方案的习题

- 习题2　设F: $\{0,1\}^m \rightarrow \{0,1\}^m$是一个抗原像攻击的函数，即对任何多项式复杂度算法
- $\mathscr{A}$, P[$\mathscr{A}$(y)输出x: y=F(x)]随m呈指数下降。基于F构造一个新的散列函数
- H：$\{0,1\}^{2m} \rightarrow \{0,1\}^m$ 如下：
- 对属于$\{0,1\}^{2m}$的任何x，首先做前后缀分割$x=u\|v$，u、v均属$\{0,1\}^m$，
- 然后输出F($u \oplus v$), 即H(x) = F($u \oplus v$).
- 试问：H是否抗原像攻击？是否抗第二类原像攻击？是否抗冲突？
- 求解概要
- (1)　H抗原像攻击
- 若H不抗原像攻击，即假若存在多项式算法A从y算出一对m位0-1串u和v，
- 使y=H($u\|v$)且A成功的概率不随m呈指数下降，但这同时也意味着y=F($u \oplus v$),
- 即$u \oplus v$是F针对y的一个原像，因此F不抗原像攻击，矛盾。
- (2)　H不抗第二类原像攻击
- 请你给出一个多项式复杂度算法$\mathscr{A}$, 从x计算出y($\neq x$)使得H(x)=H(y).
- 开动脑筋想想，实际上该算法很简单！
- (3)　H不抗冲突
- 这是(2)的普遍推论，试用抗冲突和抗第二原像攻击的定义证明之。

关于散列函数与数字签名方案的习题

- 习题3 设F: $\{0,1\}^{2m}\rightarrow\{0,1\}^m$是一个抗冲突散列函数，即对任何多项式复杂度算法
- $\mathscr{A}$, P[$\mathscr{A}$(.)输出(x,y): $y\neq x$且$F(x)=F(y)$]随m呈指数下降。
- 基于F构造一个新的散列函数H：$\{0,1\}^{4m}\rightarrow\{0,1\}^m$ 如下：
- 对属于$\{0,1\}^{4m}$的任何x，首先做前后缀分割$x=u\|v$，u、v均属于$\{0,1\}^{2m}$，
- 然后输出$F(F(u)\|F(v))$。
- 证明：H抗冲突。
- 求解概要（反证法）
- 若H不抗冲突，即假若存在多项式算法A(暂且想象以100%的概率)算出一对
- $4m$位的0-1串x和y，$y\neq x$且$H(x)=H(y)$。
- 令$x=u\|v$，$y=r\|s$，u、v、r、s均属于$\{0,1\}^{2m}$，$y\neq x$意味着$u\neq r$或者$r\neq s$；
- $H(x)=H(y)$意味着$\mathbf{F}(\ \underline{\mathbf{F}(u)\|\mathbf{F}(v)}\ ) = \mathbf{F}(\ \underline{\mathbf{F}(r)\|\mathbf{F}(s)}\ )$；
- 但F抗冲突，这意味着$F(u)\|F(v) = F(r)\|F(s)$ 以很高的概率成立（否则A必以很低的概率达成这一状态）。

  $F(u)\|F(v) = F(r)\|F(s)$意味着$\mathbf{F}(u)=\mathbf{F}(r)$并且$\mathbf{F}(v)=\mathbf{F}(s)$, 进而同理(F抗冲突)导出$u=r$并且$v=s$均以很高的概率成立。
- 然而$y\neq x$意味着$u\neq r$或者$r\neq s$ 至少有一个必然成立，这是一个矛盾。
- 综上所述，H抗冲突。
- 【基于以上的启发式分析，给出一个准确表述的证明，特别是对上述概率大小的表述，
- 换成更准确的概率不等式】

关于散列函数与数字签名方案的习题

- 习题4　设F: $\{0,1\}^{2m} \to \{0,1\}^m$是一个抗冲突散列函数，
- 仿照习题3的思路，基于F构造一个新的抗冲突散列函数
- H：$\{0,1\}^{km} \to \{0,1\}^m$，其中$k=2^t$。
- 描述H的算法，并证明H抗冲突。

【注1】上述构造是著名的*Merkel-Damgard*递归式抗冲突散列函数构造的核心。该方法从一个50%压缩率的抗冲突散列函数出发，可以造出接受任何字长（从而具有任意压缩率）的高效散列函数。

【注2】你在构造上述散列算法时，建议表达为递归形式。

关于散列函数与数字签名方案的习题

- 习题5　E是一个对称的安全加密算法，K表示其密钥。基于该对称加密
- 方案设计一个消息认证码MAC方案，其中的消息认证算法为
- $MAC_K(\mathbf{x}_1\|\mathbf{x}_2\|\ldots\|\mathbf{x}_n) = E_K(\mathbf{x}_1)\oplus E_K(\mathbf{x}_2)\ldots\oplus E_K(\mathbf{x}_n)$
- (1) 给出相应的验证算法。
- (2) 证明该MAC方案不抗伪造：
- 事实上，攻击者根据一个消息**X**及其认证码**σ**=MAC$_K$(**X**)，就能
- (通过多项式复杂度算法)生成一个消息**Y**，**X≠Y**且**σ** =MAC$_K$(**Y**)，
- 从而在完全未知密钥K的情况下伪造出一个能100%经受的起验证的
- 消息-验证码偶(**Y**, **σ**).
- 试给出一个这样的伪造/攻击。

【注】这是一个实例，说明即使采用完美的基本方案，也不必然达到安全目标。在安全协议中会看到更多的实例。因此，基于基本的安全方案构造复合安全方案，是一项复杂而微妙的工作，需要特别仔细的设计与分析。

关于散列函数与数字签名方案的习题

- 习题6 E：$\{0,1\}^m \to \{0,1\}^m$是一个对称的安全加密算法，K表示其密钥。
- 基于该对称加密方案设计一个消息认证码MAC方案，其中的消息认证
- 算法为
- $MAC_K(\mathbf{x}_1 \| \mathbf{x}_2 \| \ldots \| \mathbf{x}_n) = E_K(\mathbf{x}_1) + 3E_K(\mathbf{x}_2) + \ldots + (2n-1)E_K(\mathbf{x}_n) \bmod 2^m$.
- 以上方案将密文作为m位二进制数进行运算。
- (1) 给出相应的验证算法。
- (2) 考虑n为奇数的情形。如果限定伪造者至多只能收集2条消息及其
- 相应的认证码，但不限定消息的结构，目标是在此基础上实现100%成功
- 的伪造。你若是伪造者，将收集怎样的两条消息？并在此基础上，给出如何
- 实施伪造的方法（即根据你收集的$(\mathbf{X},\sigma_1)$和$(\mathbf{Y},\sigma_2)$ 有效算出(Z,σ_3)使得100%
- 能通过验证。当然，伪造者始终未知相应的密钥K。

【提示】$1+3+5+\ldots+(2n-1)=n^2$, 当n是奇数时，$\sigma=n^2y \bmod 2^m$对未知量可解y

- （为什么？）。思考如何利用上述数学事实、以及特殊结构的消息。

【注】这是有一个看似完美、实则失败的设计，另一方面则是一个分析攻击的好实例。

关于散列函数与数字签名方案的习题

- 习题7　考虑Schnorr签字方案，签字方采用两个非独立的随机数K_1、K_2
- 签字两个消息M_1和M_2，$K_2=2K_1+7$。试分析在什么条件下，攻击者可
- 根据这两个消息及其签字（通过多项式复杂度算法）推断出签字私钥，
- 并估计该条件发生的概率大小。

- 附：*Schnorr*签字方案(1991)：
- 公开的参数：G是q阶循环群，g是G的生成子，q是k位素数；$\boldsymbol{H}:\{0,1\}^+\rightarrow F_q$是一个抗冲突的散列函数。
- 公钥/私钥生成算法KG(k, G, g, q):
- $x\leftarrow^{\$}F_q^{\ *}$; $y\leftarrow g^{-x}$; $\boldsymbol{pk}\leftarrow y$; $\boldsymbol{sk}\leftarrow x$;
- 签名算法$Sig^H(sk, M)$, 其中sk=x:
- $K\leftarrow^{\$}F_q$; $r\leftarrow g^K$; $h\leftarrow H(\mathrm{M}\|\mathrm{r})$; $\boldsymbol{s}\leftarrow(K+xh)\ mod\ q$;
- 签名$\sigma\leftarrow(r,h,s)$。
- 验证算法Vf^H(pk, M, (r,h,s)), 其中$pk=y$:
- $h=\boldsymbol{H}(\mathrm{M}\|\mathrm{r})\wedge r=g^s y^h$;

关于散列函数与数字签名方案的习题

- 习题8　针对*Schnorr*数字签名的直接伪造尝试
- (1) 已知Schnorr方案的公钥(G,g,q,y,H)，考虑生成(M,r,h,s)使之满足
- $$h=\boldsymbol{H}(\mathrm{M}\|\mathrm{r})\wedge r=g^s y^h$$
- 的下述途径：
- 1. 选取一个消息M和一个(未必随机的) 数$\boldsymbol{r}$，并计算$\boldsymbol{h}=\mathrm{H}(M\|r)$;
- 2. 计算$\boldsymbol{a}=(y^h)^{-1}$, u^{-1}表示G的元素u在G上的逆元素；
- 3. 求一个数$\boldsymbol{s}$，使之满足$ar = g^s$。

(a)上述途径能“成功”达到伪造目的; (b)从计算复杂度的角度看，上述伪造不可能成功(!)，试解释断言(a)和(b)的理由.

- 附：*Schnorr*签字方案(1991)：
- 公开的参数：G是q阶循环群，g是G的生成子，q是k位素数；$\boldsymbol{H}$:$\{0,1\}^+\to F_q$是一个抗冲突的散列函数。
- 公钥/私钥生成算法KG(k, G, g, q): $x\leftarrow^{\$}F_q^{\ *}$; $y\leftarrow g^{-x}$; $\boldsymbol{pk}\leftarrow y$; $\boldsymbol{sk}\leftarrow x$;
- 签名算法$Sig^H(sk, M)$, 其中sk=x:
- $K\leftarrow^{\$}F_q$; $r\leftarrow g^K$; $h\leftarrow H(\mathrm{M}\|\mathrm{r})$; $s\leftarrow(K+xh) \bmod q$; 签名$\sigma\leftarrow(r,h,s)$。
- 验证算法$Vf^H(pk, \mathrm{M}, (\mathrm{r,h,s}))$, 其中$pk=y$:
- $h=\boldsymbol{H}(\mathrm{M}\|\mathrm{r})\wedge r=g^s y^h$;

关于散列函数与数字签名方案的习题

- 习题8 针对*Schnorr*数字签名的直接伪造尝试
- (1)（续） 已知公钥(G,g,q,y,H)，考虑生成(M,r,h,s)使之满足
- $$h=\boldsymbol{H}(\mathrm{M}\|\mathrm{r})\wedge r=g^s y^h$$
- 的下述途径：
- 1. 选取一个消息M和一个(未必随机的) 数$\boldsymbol{r}$，并计算$\boldsymbol{h}=\mathrm{H}(M\|r)$;
- 2.计算$\boldsymbol{a}=(y^h)^{-1}$, u^{-1}表示G的元素u在G上的逆元素；
- 3. 求一个数$\boldsymbol{s}$，使之满足$ar = g^s$。

(*a*)上述途径能“成功”达到伪造目的; (*b*)从计算复杂度的角度看, 上述伪造不可能成功(!)，试解释断言(*a*)和(*b*)的理由.

- 附：*Schnorr*签字方案(1991)：
- 公开的参数：G是q阶循环群，g是G的生成子，q是k位素数；$\boldsymbol{H}$:$\{0,1\}^+\rightarrow F_q$是一个抗冲突的散列函数。
- 公钥/私钥生成算法KG(*k*, *G*, g, q): $x\leftarrow^{\$}F_q^*$; $y\leftarrow g^{-x}$; $\boldsymbol{pk}\leftarrow y$; $\boldsymbol{sk}\leftarrow x$;
- 签名算法$Sig^H(sk, M)$, 其中sk=x:
- $K\leftarrow^{\$}F_q$; $r\leftarrow g^K$; $h\leftarrow H(\mathrm{M}\|\mathrm{r})$; $s\leftarrow(K+xh) \bmod q$; 签名$\sigma\leftarrow(r,h,s)$。
- 验证算法$Vf^H(pk, \mathrm{M}, (\mathrm{r,h,s}))$, 其中$pk=y$:
- $h=\boldsymbol{H}(\mathrm{M}\|\mathrm{r})\wedge r=g^s y^h$;

关于散列函数与数字签名方案的习题

- 习题8　针对*Schnorr*数字签名的直接伪造尝试
- (2) 已知Schnorr方案的公钥(G,g,q,y,H)，考虑生成(M,r,h,s)使之满足
- $$h=\boldsymbol{H}(\mathrm{M}\|\mathrm{r})\wedge \boldsymbol{r}=g^s y^h$$
- 的下述途径：
- 1. 选取一对整数$\boldsymbol{s}$和$\boldsymbol{h}$，计算$\boldsymbol{r}=g^s y^h$；
- 2. 求一个消息$\boldsymbol{M}$，使之满足$h=\mathrm{H}(M\|r)$；

(*a*)上述途径能“成功”达到伪造的目的; (*b*)从计算复杂度的角度看，上述伪造不可能成功(!)，试解释断言(*a*)和(*b*)的理由.

- 附：*Schnorr*签字方案(1991)：
- 公开的参数：G是q阶循环群，g是G的生成子，q是k位素数；$\boldsymbol{H}:\{0,1\}^+\to F_q$是一个抗冲突的散列函数。
- 公钥/私钥生成算法KG(k, G, g, q):　$x\leftarrow^{\$}F_q^*$; $y\leftarrow g^{-x}$; $\boldsymbol{pk}\leftarrow y$; $\boldsymbol{sk}\leftarrow x$;
- 签名算法$Sig^H(sk, M)$, 其中sk=x:
- $K\leftarrow^{\$}F_q$; $\boldsymbol{r}\leftarrow g^K$; $\boldsymbol{h}\leftarrow H(\mathrm{M}\|\mathrm{r})$; $\boldsymbol{s}\leftarrow(K+xh) \bmod q$;　签名$\sigma\leftarrow(r,h,s)$。
- 验证算法$Vf^H(pk, \mathrm{M}, (\mathrm{r,h,s}))$, 其中$pk$=y:
- $h=\boldsymbol{H}(\mathrm{M}\|\mathrm{r})\wedge r=g^s y^h$;

关于散列函数与数字签名方案的习题

- 习题8　针对*Schnorr*数字签名的直接伪造尝试
- (3) 已知Schnorr方案的公钥(G,g,q,y,H)，考虑生成(M,r,h,s)使之满足
- $h=\boldsymbol{H}(\mathrm{M}\|\mathrm{r})\wedge r=g^s y^h$
- 的下述途径：
- 1. 选取一对整数s和h，计算$r = g^s y^h$；
- 2. 求一个消息M，计算$h^*= \mathrm{H}(M\|r)$;
- 3. 如果$h^*\neq h$ 则返回步骤1，重新生成s和h进行计算，直到有$h^*=h$。

(*a*)上述途径能"成功"达到伪造的目的; (*b*)从计算复杂度的角度看, 上述伪造仍不可能成功(!)，试解释断言(*a*)和(*b*)的理由.

- 附：*Schnorr*签字方案(1991)：
- 公开的参数：G是q阶循环群，g是G的生成子，q是k位素数；$\boldsymbol{H}:\{0,1\}^+\rightarrow F_q$是一个抗冲突的散列函数。
- 公钥/私钥生成算法KG(k, G, g, q):　$x\leftarrow^{\$}F_q^{\,*}$; $y\leftarrow g^{-x}$; $\boldsymbol{pk}\leftarrow y$; $\boldsymbol{sk}\leftarrow x$;
- 签名算法$Sig^H(sk, M)$, 其中sk=x:
- $K\leftarrow^{\$}F_q$; $r\leftarrow g^K$; $h\leftarrow H(\mathrm{M}\|\mathrm{r})$; $s\leftarrow(K+xh) \bmod q$; 签名$\sigma\leftarrow(r,h,s)$。
- 验证算法$Vf^H(pk, \mathrm{M}, (\mathrm{r,h,s}))$, 其中$pk$=$y$:
- $h=\boldsymbol{H}(\mathrm{M}\|\mathrm{r})\wedge r=g^s y^h$;

关于散列函数与数字签名方案的习题

- 思考题（不提交）
- Stallings教程第六版：
- 11.2(a)(b)、11.3(a)(b)、11.6；
- 12.3、12.4、12.9（这三题在阅读第十二章相应的小节后思考）
- 13.7(一个设计错误的签字方案).

下单元内容预告：典型安全协议

-

1