计算机密码学理论与技术

RSA和OAEP/RSA方案

田园

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

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

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

公钥加密方案(1)

内容提要

- 一、基于因子分解难解性的公钥加密方案：Stallings 教程9.1~9.2
- (1) ***RSA***方案：基本工作原理
- (2) ***RSA***方案：更多的认识
- (3) IT业界标准：***OAEP/RSA***方案
- 二、基于离散对数问题难解性的公钥加密方案
- (4) *ElGamal*方案 Stallings 10.2
- (5) *Cramer-Shoup*方案+ +表示补充的内容，参考补充的电子讲义第8章
- 三、公钥加密方案的精确的安全模型和安全定义+
- 四、混合加密方案+
- Fujisaki-Okamato、GERM等；
- 五、***IBE***加密方案(*Bohen-Franklin*，*Walters*等) +

公钥加密方案(2)

RSA：基于因子分解难解性的公钥加密方案：

- 学习要点
- (1) ***RSA***方案：基本工作原理
- (2) ***RSA***方案：更多的认识
- 参数生成；
- 不正确的应用；
- 密文可塑性；
- (3) IT业界标准：***OAEP/RSA***方案
- 随机Oracle；
- Bellare-Rogaway方案
-

公钥加密方案(3)

- (1)RSA 公钥-私钥生成算法
- 生成大的素数p, q(p≠q)；
- 计算整数N=pq；
- 计算*Euler*函数ϕ(N)=(p-1)(q-1)；
- 生成一个奇整数e：(e,ϕ(N))=1；
- 计算整数d：ed=1 mod ϕ(N)
- (注：条件(e,ϕ(N))=1保证同余方程确实有解d)。
- RSA公钥pk=(N,e), RSA私钥sk=(d,p,q)。
- (注：素数***p***、***q***不再需要，但不能泄露！)
- (2) RSA加密算法E(pk,M)
- 对任何明文M: 1≦M≦N-1，生成密文$\boldsymbol{y} = M^e \bmod N$。
- (3) RSA解密算法D(sk,y)
- 对密文y，计算$M = y^d \bmod N$。

公钥加密方案(4)

例：(1)RSA 公钥-私钥生成算法

- 生成素数p=3, q=7($p \neq q$)；
- 计算整数N=pq=21；
- 计算$Euler$函数$\varphi(N)=(p-1)(q-1)=12$；
- 生成一个奇整数e=5：(e,ϕ(N))=1；
- 计算整数d：5d= 1 mod 12, 故d=5；
- RSA公钥pk=(N,e)=(21,5), RSA私钥sk=(d)=(5)。
- (2) RSA加密算法E(pk,M)
- 对明文M=2:，生成密文$y = M^e \bmod N = 2^5 \bmod 21 = \underline{11}$；
- 对明文M=3:，生成密文$y = 3^5 \bmod 21 = -\ \underline{9}$；
- (3) RSA解密算法D(sk,y)
- 对密文y=11，计算
- $y^d \bmod N = 11^5 \bmod 21$
- $= 11^5 = 11^2 \cdot 11^2 \cdot 11 = 16 \cdot 16 \cdot 11 = (-5)(-5)11 = 25 \cdot 11 = 4 \cdot 11 = 2 \bmod 21$；
- 【习题】对密文$y = -9$，验证$y^d \bmod N = 3$.

公钥加密方案(5)

- **RSA解密算法的正确性证明**

第一种情形：$(M, N)=1$

这时的解密计算

$$y^d \bmod N = M^{ed} \bmod N = M^{1+k\varphi(N)} \bmod N$$

$$= M\,(M^{\varphi(N)} \bmod N)^k \bmod N = M \bmod N = M。$$

- 第二种情形：$(M, N)\neq 1$
- 这时必有$(M,N)=p$或q。若$(M,N)=p$，则必有$M=Ap$且$(A,q)=1$，
- 因此 $y^d \bmod p = (Ap)^{ed} \bmod p = 0 = M \bmod p$;
- $y^d \bmod q = (Ap)^{ed} \bmod q = (Ap)^{1+k\varphi(N)} \bmod q$
- $= (Ap)^{1+k(p-1)(q-1)} \bmod q = ((Ap)^{q-1} \bmod q)^{k(p-1)} Ap \bmod q = Ap \bmod q$;
- 即 $y^d \bmod p = M \bmod p$、 $y^d \bmod q = M \bmod q$，进而(注意$pq=N$)
- 根据中国余数定理有 $y^d \bmod N = M \bmod N = M$。
- 综上所述，$y^d \bmod N = M$恒成立。

公钥加密方案(6)

- RSA方案的安全性
-
- 基本事实
- 仅仅基于公开的信息e和N，不存在现实可行的算法A计算出$\varphi(N)$，
- 因此也无法推算出用以解密的私钥d。
- 更多的认识
- 一、素数p和q的要求
- (1) p和q是不同的素数，并且$p=2p^*+1$, $q=2q^*+1$, 其中p^*和q^*也是素数。
- (2) p和q是大素数，根据当前计算能力对安全性要求的推算，
- 若p和q为1000位素数，并假设每秒钟测试10^{20}次(一万亿亿)解密，
- 注意到 $N \sim 2^{2000} \sim \varphi(N)$，私钥$d$数量 $= \varphi(\varphi(N)) \sim 2^{1000}$
- 1天~8万秒；3年~ 3×365×8万~ 10^8秒，
- 尝试完全部私钥需要的时间 $\sim (2^{1000}/ 10^{20}) \sim 2^{940} \sim 2^{910}$年
- $\sim 2^{850}$倍宇宙年龄！

公钥加密方案(7)

- RSA方案的安全性
- 更多的认识

- 二、对RSA<u>不正确</u>的使用（例一）
- 设想一组用户，其*RSA*模数相同、均等于*N*且公钥 *e*彼此互素，
- 若某个发送者A需将同一个消息*M*分别发送给B和C，于是A生成两个密文$y_B=M^{e_B} \bmod N$和$y_C=M^{e_C} \bmod N$。
- 攻击者X截获到y_B和y_C后，能容易地计算出来*M*。
- 原因：既然e_B和e_c公开且互素，攻击者A可由Euclid算法计算出整数u和v，使之满足$e_Bu+e_Cv=(e_B, e_C)=1$，进而计算
- $$y_B^u y_C^v \bmod N = M^{e_Bu+e_Cv} \bmod N = M\,!$$
-
- 结论：在应用RSA方案时，不同的合法解密者应持有不同的公钥模数*N*且另一个公钥分量*e* 不应该彼此互素。
- 该结论对OAEP/RSA同样正确。

公钥加密方案(8)

- *RSA*方案的安全性
- 更多的认识
- 二、对*RSA*不正确的使用（例二）
- 设想三个用户A、B、C分别持有RSA公钥参数$e_A=e_B=e_C=3$, N_A、N_B、
- N_C彼此不同且互素。如果某用户U向A、B、C广播消息M，相应的RSA
- 密文是：$y_A= M^3 \bmod N_A$，$y_B = M^3 \bmod N_B$，$y_C = M^3 \bmod N_C$
- 攻击者基于密文y_A、y_B、y_C和公开信息，应用中国余数定理求解$\boldsymbol{x}$：
- $x = y_A \bmod N_A$，$x = y_B \bmod N_B$，$x = y_C \bmod N_C$，
- 再计算x的三次方根，就可以准确恢复M！

- 结论：RSA方案仅适用于点-点通信，不能保证广播或组群通信的安全。

公钥加密方案(9)

• *RSA*方案的安全性

- 更多的认识
- 三、**密文可塑性**(Cyphertext Malleability：实例之一)
- 考虑以下过程：
- 1. ***A***用***B***的RSA公钥(e, N)生成密文：$\boldsymbol{y} = M^e \bmod N$；
- 2. ***X***在中途截获***y***，用自行生成的正数a计算
- $$y^* = y a^e \bmod N$$
- 3. ***X***将**y***继续发向***B***;
- 4. ***B***接收到***y****，做解密计算 $y^{*d} \bmod N$结果$= aM \bmod N$。
- 实例：
- N=很大的整数，明文M =10000是A向主管B所指示的X的应发工资，X采用参数
- a =10，于是B最终收到的工资指令= 10M *mod N*= 10M！(注意M远小于N)

公钥加密方案(10)

- *RSA*方案的安全性
-
- 更多的认识
- 三、**密文可塑性**(实例之二)
- 考虑以下过程：
- 1. ***A***用***B***的RSA公钥(e,N)生成密文：$\boldsymbol{y} = M^e \bmod N$；
- 2. ***X***在中途截获***y***，用自行生成的正数***t***计算
- $$\boldsymbol{y}^* = y^t \bmod N$$
- 3. ***X***将$\mathbf{y}^*$继续发向***B***;
- 4. ***B***接收到$\boldsymbol{y}^*$，做解密计算 $y^{*d} \bmod N$结果$= M^t mod\ N$。
-
- 密文可塑性(实例之三，习题)
-
- 试用M的密文y生成同原始明文具有关系$M^*=aM^t$的密文。
-

公钥加密方案(11)

- *RSA*方案的安全性

- (1) 密文可塑性对某些应用而言无疑是一种安全缺陷。
- (2) 密文可塑性不同于明文泄露意义上的安全缺陷：
- 密文可塑性并不意味着加密方案泄露任何明文信息，
- 而是意味着攻击者可以仅借助于公开信息实现对密文的有效变换，
- 使变换前、后的明文具有攻击者所决定的特定关系(如$M^* = aM$ 等)，
- 但攻击者既无法破译M也无法破译M^*。
- (3) 修定RSA方案以消除其密文可塑性缺陷的改进方案：
- OAEP/RSA(1993, M.Bellare & P.Rogaway;
- 1999, J.Stern & Okamato)
- Bellare et al, *Optimal Asymmetric Encryption - How to Encrypt with RSA, 1995.*
- *Mao W Modern Cryptology and Applications*，电子工业出版社，2005.
- 田园著 计算机密码学-通用方案构造与安全证明，电子工业出版社，2008.

公钥加密方案(12)

- *OAEP/RSA*方案：方案描述（参考Stalling 图9.10）

- (1)公钥-私钥生成算法：
- **G**、***H***是两个随机散列函数，输出分别为$n+k^o$位和位k^o二进制数；
- ***N***是两个大素数的乘积、$n+2k^o$位二进制数；
- ***e***是和$\phi(N)$互素的一个正整数，
- ***d***是满足方程$ed=1 \bmod \phi(N)$的一个正整数；
- 公钥***pk***$=(e,N,H,G)$；私钥***sk***$=d$；

- 注1：符号x||y表示两个字串x和y的联结；
- 注2：一个对象有时被作为一个数，有时则作为一个纯粹的字串，这在上下文中是清楚的，请注意区别。

- (2)加密算法E(pk, M)，其中明文M是n位二进制数：
- 随机选取一个k^o位二进制数**r**;
- **s**$\leftarrow(M||r)\oplus G(r)$; /*按位异或*/
- **t**$\leftarrow r\oplus H(s)$; /*按位异或*/
- **y**$\leftarrow(s||t)^e \bmod N$;
- output(y);　　注3：以上加密算法是随机算法。

(3)解密算法D(sk, y):
- **x**$\leftarrow y^d \bmod N$;
- 分解x 的前后缀结构：**x** = s||t, |s|= n+k, |t|=k;
- **r**$\leftarrow t\oplus H(s)$;
- **M***$\leftarrow s\oplus G(r)$;
- if **M*=M||r** /* 检验M*的最低k位是否等于 r */
- then output(M); /* 将M*的最高$n+k^o$位作为解密的明文 */ else output(“错误”);

公钥加密方案(13)

- *OAEP/RSA*方案：**随机Oracle**

- 随机Oracle H是一个函数/映射，不存在多项式复杂度算法能够
- 基于其历史样本对其新的输入-输出进行有效的预测，即
- 对任何概率性多项式时间复杂度算法A，对任何多项式函数
- $n=poly(k)$，恒成立
- $P[A(\{(\boldsymbol{x}_i, \boldsymbol{y}_i): \boldsymbol{y}_i=H(\boldsymbol{x}_i), i=1,\ldots,n\}, \langle H\rangle, \boldsymbol{x}) = H(\boldsymbol{x})] = O(2^{-k})$
- 注：<H>表示H的算法代码，因此Oracle的不可预测性不依赖于隐藏
- H本身的算法，而是依赖于H的内在性质。

公钥加密方案(14)

- *OAEP/RSA*方案：**安全性质**

- *OAEP/RSA*方案的安全性建立在以下条件上：

- (1) 不存在计算**Euler**函数值的多项式复杂度算法；

- (2) *G*和*H*是随机Oracle且独立；

- *Bellware-Rogaway-Stern-Okamato*定理(1999)：
- 在以上条件下，*OAEP/RSA*方案具有保密性且抗密文可塑。

公钥加密方案(15)

- 习题：研讨以下公钥加密方案

8-22(*Paillier-Damgard-Catalano*公钥加密方案,1999,2000,2002) 设$N=p_1p_2$是有两个大素因子的RSA模数，正整数$s<p_1,p_2$，首先我们接受一条普遍性质：在模N^{s+1}的乘法群$Z^*_{N^{s+1}}$中 1+N的阶为N^S。以下讨论涉及s=1 的情形。公钥pk=RSA公钥(e,N)；私钥$sk=d$，其中$ed=1\bmod \varphi(N)$；明文$m\in Z_N$；加密算法$E(pk, m)$输出密文$y\leftarrow(1+mN)r^e \bmod N^2$，其中$r\xleftarrow{\$}Z^*_N$；对密文$y$的解密运算如下：$r\leftarrow y^d \bmod N$; $m\leftarrow((r^{-e}y-1)\bmod N^2)/N$。已经证明：若N上的所谓判定性$e$-次剩余问题难解，则以上方案保密。

(1) 验证以上加密算法是正确的，即满足一致性条件；

(2) 验证以上方案具有同态性质：$E(pk, m_1)E(pk, m_2)= E(pk, (m_1+m_2)\bmod N) \bmod N^2$。

注：同态性质使这一方案密文可塑，因此作为纯粹的加密方案并不可取。*Paillier-Damgard-Catalano* 公钥加密方案的真正用途在于作为构造许多复杂安全协议的工具，在这方面其同态性质具有重要应用。

习题

- Stalling教程
- 习题9.2、9.3、9.4、9.6、
- 9.7（答案：不安全；为什么？）
- 9.8（答案：不安全；想想这样的加密方法能否掩盖
- 明文的上下文特征（任何可用来实施破译的特征）？
- 这个例子告诉我们，安全的加密方案需要用到正确的明文
- 粒度上，例如字符粒度的安全不等于全文粒度上的安全，
- 这一点和对称（分组）加密必须结合密文模式(mode)来使用，
- 道理是一样的，两者结合才能保证文全局性的安全性）