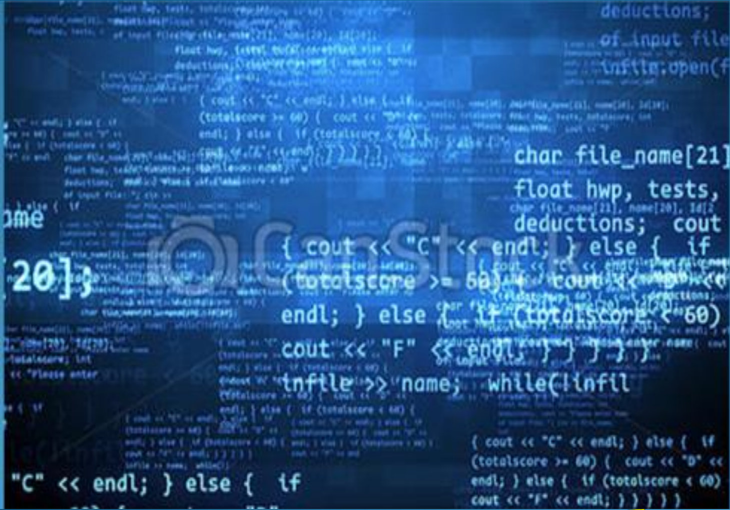

密码学理论与技术

公钥加密方案的安全模型

*ElGamal*公钥加密方案

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：
- (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
- (5) *Cramer-Shoup*方案
- 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
- 五、***IBE***加密方案(*Bohen-Franklin*)

公钥加密方案(2)

- 基于离散对数问题难解性的公钥加密方案
- ***ElGamal***方案(1985)：算法(参阅Stallings 10.2)
  - G是素q阶循环群，例如G=乘法群F_q^*，生成子为g：（即$G=\{e,g,g^2,\ldots,g^{q-1}\}$)
  - 密钥生成算法KG(q,g):
  - $\boldsymbol{x} \leftarrow^{\$} F_q$; $\boldsymbol{Y} \leftarrow g^x$;
  - 公钥$\boldsymbol{pk} \leftarrow (q,g,Y)$;私钥$\boldsymbol{sk} \leftarrow (x)$;
  - 加密算法E(pk, M), $M \in G$:
  - $\boldsymbol{r} \leftarrow^{\$} F_q$; $\boldsymbol{R} \leftarrow \boldsymbol{g}^r$; $\boldsymbol{T} \leftarrow Y^r$; $\boldsymbol{W} \leftarrow \boldsymbol{TM}$; output(R, W);
  - 解密算法D$(sk, (R,W))$:
  - $\boldsymbol{T} \leftarrow R^x$; $\boldsymbol{M} \leftarrow WT^{-1}$; output(M);

公钥加密方案(3)

- ***ElGamal***方案(1985)： 解密算法的正确性

- G是素q阶循环群，生成子为g： （即$G=\{e,g,g^2,\ldots,g^{q-1}\}$）
- 密钥生成算法KG(q,g):
- $\boldsymbol{x} \leftarrow^{\$} F_q$; $\boldsymbol{Y} \leftarrow g^x$; 公钥$\boldsymbol{pk}$=($q$,$g$,$Y$);私钥$\boldsymbol{sk}$=($x$);
- 加密算法E(pk, M), $M \in G$:
- $\boldsymbol{r} \leftarrow^{\$} F_q$; $\boldsymbol{R} \leftarrow \boldsymbol{g}^r$; $\boldsymbol{T} \leftarrow Y^r$; $\boldsymbol{W} \leftarrow \boldsymbol{TM}$; output(R, W);
- 解密算法D(sk, (R,W)):
- $\boldsymbol{T_1} \leftarrow R^x$; $\boldsymbol{M} \leftarrow WT_1^{-1}$; output(M);

- $T_1 = R^x = (g^r)^x = (g^x)^r = Y^r$, 因此
- $WT_1^{-1} = (TM)T_1^{-1} = (Y^rM)(Y^r)^{-1} = M$ =明文。

【注】再次注意，这里的加密算法是随机算法！

公钥加密方案(4)

- ***ElGamal***方案：安全性和密文可塑性

- 一、直观的结论：若循环群G上的离散对数问题难解，
- 则*ElGamal*方案具有密文保密性。

- 二、对明文M，*ElGamal*方案的合法密文C = (y_1,y_2), $y_1=g^r$, $y_2=g^{xr}M$。验证：
- (1) 对任何$a\in\mathcal{G}$，$y^* = (y_1,ay_2)$是一个合法的密文，且解密出的明文
- 将是 $\boldsymbol{aM}$;
- (2) 对任何整数常数b，$y^*=(y_1^b,y_2^b)$ 是一个合法的密文，且解密出
- 的明文将是 $\boldsymbol{M^b}$;
- (3) 对任何常数$a\in\mathcal{G}$和整数常数b，$y^* = (y_1^b,ay_2^b)$是一个合法的密文，
- 且解密出的明文将是$\boldsymbol{aM^b}$。
- 分　析
- (1) $\boldsymbol{y_1 = g^r,\ ay_2 = ag^{xr}M = g^{xr}(aM)}$。
- (2) $\boldsymbol{y_1^b = g^{rb},\ y_2^b = g^{xrb}M^b}$ 。

公钥加密方案(5)

- 公钥加密方案普适**安全模型**: (KG,E,D)的**CPA-安全**

P： 解密私钥持有者　　***k***是安全参数　　A： 破译者/P.P.T算法

1. $(pk,sk) \leftarrow KG(k)$

2. pk （P → A）

3. $(St,M_0,M_1) \leftarrow A1(pk)$:
$|M_0|=|M_1|$且 $M_0 \neq M_1$

4. M_0,M_1 （A → P）

5. $b \leftarrow^{\$} \{0,1\}$;
$\mathbf{y}^* \leftarrow E(pk,M_b)$;

6. $\mathbf{y}^*$ （P → A）

7. $b^* \leftarrow A_2(\mathbf{y}^*, St)$:

安全的加密算法犹如高明的化妆师，拿手好戏是掩饰。

- 公钥加密方案定义做**CPA-安全**(*Secure Against Chosen Plaintext Attack*)，若存在常数$a>0$和$b>0$，对$k \rightarrow \infty$满足
- $$|P[b^*= b] - ½| \leqq \mathbf{a}2^{-bk}$$

【思考】如果加密算法E是确定性算法，以上的过程中A成功的概率是多少？　　答案：P[b*=b]=1！

公钥加密方案(6)

- 公钥加密方案普适**安全模型**: (KG,E,D)的**CCA-安全**

P：解密私钥持有者　　k是安全参数　　**A**：破译者/P.P.T算法

1. $(pk,sk) \leftarrow KG(k)$
2. pk （P → A）
3. $(St_1,\{y_k\}_{k=1\ldots N1}) \leftarrow A_1(pk)$: y_k是该方案的一组密文
4. $\{y_k\}_{k=1\ldots N1}$ （A → P）
5. $U_k \leftarrow D(sk,y_k)$
6. $\{U_k\}_{k=1\ldots N1}$ （P → A）
7. $(St_2,M_0,M_1) \leftarrow A_2(St_1,\{U_k\})$: $|M_0|=|M_1|$、$M_0 \neq M_1$ 且M_0,M_1不属于$\{U_k\}$
8. M_0,M_1 （A → P）
9. $b \leftarrow^{\$} \{0,1\}$; $\mathbf{y}^* \leftarrow E(pk,M_b)$;
10. $\mathbf{y}^*$ （P → A）
11. $(St_3,\{z_k\}_{k=1\ldots N2}) \leftarrow A_3(\mathbf{y}^*, St_2)$: z_k是该方案的一组密文
12. $\{z_k\}_{k=1\ldots N2}$ （A → P）
13. $V_k \leftarrow D(sk,z_k)$
14. $\{V_k\}_{k=1\ldots N2}$ （P → A）
15. $b^* \leftarrow A_4(\mathbf{y}^*, St_3, \{V_k\})$

- 公钥加密方案定义做**CCA-安全**(*Secure Against Chosen Cyphertext Attack*)，若存在常数$a>0$和$b>0$，对$k\rightarrow\infty$满足

$$|P[b^* = b] - ½| \leqq a2^{-bk}$$

习题

- 10.6(a)和(b)。

公钥加密方案(7)

- 公钥加密方案普适安全模型：主要结论

- CPA-安全：语义安全/抗选择明文攻击
- CCA-安全：抗选择密文攻击
- CMA-安全：抗密文可塑性安全
- (1) **CPA-安全 < CCA-安全 = CMA-安全。**
- 原始论文：M. Bellare, A. Desai, D. Pointcheval, P. Rogaway, *Relations among notions of security for public-key encryption schemes*, Lecture Notes in Computer Science, vol. 1462, 1998, pp. 26–45.

- (2) 一个公钥加密方案若是CPA安全的，则加密算法必是随机算法。

- (3) 一个公钥加密方案若是CPA安全的，则任何*P.P.T*算法成功破译任何密文
- 的概率随安全参数$k\to\infty$的渐进上界为$O(2^{-bk})$, $b>0$是某个常数。

【习题】证明若安全方案是CCA-安全的则必为CCA-安全则

证明命题(3)。

公钥加密方案(8)

- 公钥加密方案的普适安全模型：小 结
- 任何安全模型均须反映以下要素：
- (1) 安全方案户欧协议的工作特点
- (2) 攻击者的能力：**P.P.T算法**
- (3) 实施攻击时可能获取到的信息
- (4) 攻击者的目标：破译、伪造、身份欺诈....
- (5) 攻击者达成其攻击目标程度的度量：
- 攻击成功的概率随安全参数的渐进速降

公钥加密方案(9)

- ***ElGamal***方案：精确的安全性结论
- 记号：$poly(k)$表示k的某个多项式。
- 若群族
- $\{G_{g(k),q(k)}: G_{g(k),q(k)}$是以$g(k)$为生成子的素$q(k)$阶循环群，$k\to \infty\}$
- 上的判定性*Diffie-Hellman*问题难解，即任何*P.P.T*算法(平均时间
- 复杂度是$poly(k)$的随机算法)***A***都有
- $| P[A(g(k), u,v,w) = 1|1\leqq x,y\leqq q(k), u=g(k)^x, v=g(k)^y, w=g(k)^{xy}]$
- $- P[A(g(k), u,v,w) = 1|1\leqq x,y,w\leqq q(k), u=g(k)^x, v=g(k)^y, w=g(k)^w]|$
- $\leqq O(2^{-k})$， $k\to \infty$，
- 则*ElGamal*方案具有语义安全性。