Generalizations of RSA Public Key Cryptosystem *

Banghe Li

July 20, 2005

Abstract

In this paper, for given $N = pq$ with p and q different odd primes, and $m = 1, 2, \cdots$, we give a public key cryptosystem. When $m = 1$ the system is just the famous RSA system. And when $m \geq 2$, the system is usually more secure than the one with $m = 1$.

1 Introduction

In this paper, we present a series of generalizations of the famous RSA public key cryptosystem (cf.[1],[2]), they are more secure in general.

Let n be a positive integer, $\mathbb{Z}_n{}^*$ be the group of invertible elements in $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$. RSA crytosystem works on $\mathbb{Z}_n{}^*$.

Let A be a commutative ring with identity element 1, $P = x^m + a_1x^{m-1} + a_{m-1}x + a_m \in A[x]$. Denote by A_P the quotient ring $A[x]/P$, and A_P^* the group of invertible elements in A_P. For $A = \mathbb{Z}_n$, we use $\mathbb{Z}_{n,P}$ to replace $(\mathbb{Z}_n)_P$. Thus our cryptosystems work on $\mathbb{Z}_{n,P}^*$, and when $P = x + a \in \mathbb{Z}_n[x]$, $\mathbb{Z}_{n,P}^* = \mathbb{Z}_n^*$, our cryptosystem is the same as RSA.

RSA took $N = pq$, where p, q are big primes. For such N, we call $P = x^m + a_1x^{m-1} + \cdots + a_m \in \mathbb{Z}_n[x]$ to be special to N if P mod p and P mod q are irreducible over the fields F_p and F_q respectively. The number of the elements in $\mathbb{Z}_{N,P}^*$ denoted by $\phi(N, P)$ will be proved to be $(p^m - 1)(q^m - 1)$.

For general P, $\phi(N, P)$ depends also on $a_1, \cdots, a_m$ and is usually very difficult to calculate, since it concerns solving congruence equations of degree m. For $m = 2$, the formula for $\phi(N, P)$ is given in section 2.

In our generalizations of the RSA system, public key K is (N, P, e), where $e \in \{2, 3, \cdots, \phi(N, P) - 2\}$ with $\gcd(e, \phi(N, P)) = 1$ can be randomly chosen, and $d \in$

*This research is partially supported by 973 projects (2004CB318000)

$\{2, \cdots, \phi(N,P)-2\}$ with

$$ed \equiv 1 \bmod \phi(N,P)$$

is the secret key. Notice that any element in $\mathbb{Z}_{N,P}$ is uniquely expressed as

$$y = b_1 x^{m-1} + b_2 x^{m-2} + \cdots + b_m \qquad (1)$$

with $b_i \in \mathbb{Z}_N$. $y^e \bmod P$ can be calculated on computer, by e.g. the software package "Powmod" in Maple. Thus the encryption and decryption function ϵ, δ: $\mathbb{Z}_{N,P}^* \to \mathbb{Z}_{N,P}^*$ are defined by

$$\epsilon(y) = y^e, \delta(y) = y^d$$

.

Since the order of any element in $\mathbb{Z}_{N,P}^*$ is a divisor of $\phi(N,P)$, $y^{\phi(N,P)} = 1$ in $\mathbb{Z}_{N,P}$. Thus

$$y^{ed} = y \in \mathbb{Z}_{N,P}^*$$

In the case of P being special to N, we will prove that $y^{ed} = y$ is actually true for any $y \in \mathbb{Z}_{N,P}$.

For any $y \in \mathbb{Z}_{N,P}$ with P special to N, there exists a smallest positive integer β such that

$$y^{e^\beta} = y \in \mathbb{Z}_{N,P}$$

We call β the Simmons period of y in $\mathbb{Z}_{N,P}$ with respect to e . Note that $\mathbb{Z}_N^*$ is a subgroup of $\mathbb{Z}_{N,P}^*$ consisting of elements y in the form (1) with $b_1 = \cdots = b_{m-1} = 0$, $b_m \in \mathbb{Z}_N^*$. The number of the elements of the quotient group $\mathbb{Z}_{N,P}^*/\mathbb{Z}_N^*$ is

$$(p^m-1)(q^m-1)/(p-1)(q-1) = (p^{m-1}+p^{m-2}+\cdots+1)(q^{m-1}+q^{m-2}+\cdots+1)$$

Especially when $m = 2$, this number is $(p+1)(q+1)$.

In RSA system, to prevent the Simmons attack, one has to choose p and q to make Simmons period big enough, e.g. to let $p-1$ and $q-1$ having big prime factors. Now we see that if $y \in \mathbb{Z}_{N,P}^* - \mathbb{Z}_N^*$, the Simmons period of y will be usually much bigger than those of the elements in $\mathbb{Z}_N^*$. To ensure this, we may require $p^{m-1} + \cdots + 1$ and $q^{m-1} + \cdots + 1$ to have big prime factors.

In the practice of using RSA system, to ensure the security, one has to choose big primes p, q and e to satisfy certain additional conditions. This is not easy. While for us, when p and q are fixed (they may not satisfy some additional conditions), we can just choose suitable m to increase the security, e.g. increasing the Simmons period.

Notice that in the case of P special to N, $\phi(N,P)$ can be replaced by any common multiple M of $p^m - 1$ and $q^m - 1$, and

$$ed \equiv 1 \bmod M$$

When $M < \phi(N,P)$, the calculation of d from e should be easier.

2 Theoretic Preparations

Let A be a unital commutative ring, $A[x]$ be the polynomial ring over A with one variable x. For any $P = x^m + a_1x^{m-1} + \cdots + a_m \in A[x]$, any element of the quotient ring $A_P = A[x]/P$ is uniquely expressed as $y_1x^{m-1} + y_2x^{m-2} + \cdots + y_m$. So A_P is a free module over A with $1, x, \cdots, x^{m-1}$ as a free basis.

Let $b = b_1x^{m-1} + b_2x^{m-2} + \cdots + b_m \in A_P$. We define a map

$$M_b : A_P \to A_P$$

given by $M_b(y) = by$, where by is the product of b and y in the ring A_P.

It is easily seen that M_b is a linear transformation of A_P as A-module. Writing $M_b(y)$ as $y'_1x^{m-1} + y'_2x^{m-2} + \cdots + y'_m$, then

$$\begin{pmatrix} y'_1 \\ \cdots \\ y'_m \end{pmatrix} = \begin{pmatrix} b_{11} & \cdots & b_{1m} \\ \cdots & \cdots & \cdots \\ b_{m1} & \cdots & b_{mm} \end{pmatrix} \begin{pmatrix} y_1 \\ \cdots \\ y_m \end{pmatrix} \tag{2}$$

where $b_{ij} \in A$. By abuse of notations, we use still M_b to denote the matrix (b_{ij}), and $|M_b|$ the determinant of M_b. Let A_P^* be the group of invertible elements in A_P. We have

Lemma 1. $b \in A_P$ is in A_P^* iff $|M_b| \in A^*$.

Proof. b being in A_P^* implies that there is a $c \in A_P$ such that $bc = 1$. Thus M_bM_c is the identity matrix, hence $|M_b||M_c| = 1$, and $|M_b| \in A^*$.

Now assume $|M_b| \in A^*$. Substitute $y'_1 = \cdots = y'_{m-1} = 0$, and $y'_m = 1$ into (2), we get an equation on the variable $y_1, \cdots, y_m$:

$$(0, \cdots, 0, 1)^T = M_b(y_1, \cdots, y_m)^T$$

$|M_b| \in A^*$ implies that there is an $m \times m$ matrix M_b^{-1} with entries in A such that $M_bM_b^{-1}$ is the $m \times m$ identity matrix.

Let $M_b^{-1}(0, \cdots, 0, 1)^T = (c_1, \cdots, c_m)^T$. Then $c = c_1x^{m-1} + c_2x^{m-2} + \cdots + c_m$ is the inverse of b in A_P. Hence $b \in A_P^*$. The lemma is proved.

For $P = x^2 + a_1x + a_2$, $b = b_1x + b_2$, we have $-M_b = b_2^2 - a_1b_1b_2 + a_2b_1^2$.

Let $N = pq$ with p and q different odd prime. When $a \not\equiv 0 \bmod p$, let $(\frac{a}{p})$ be the Legendre symbol. We introduce the following notations:

$$\Delta_p = \begin{cases} 0, & \text{if } \frac{(N+1)^2}{4}a_1^2 \equiv a_2 \bmod p \\ \left(\frac{\frac{(N+1)^2}{4}a_1^2 - a_2}{p}\right), & \text{otherwise} \end{cases}$$

$$\Delta_q = \begin{cases} 0, & \text{if } \frac{(N+1)^2}{4}a_1^2 \equiv a_2 \bmod q \\ \left(\frac{\frac{(N+1)^2}{4}a_1^2 - a_2}{q}\right), & \text{otherwise} \end{cases}$$

Then we have

Proposition 1. Let P and N be as above, then

$$\phi(N,P)=\begin{cases}(p^2-1)(q^2-1), & \text{if}\Delta_p=\Delta_q=-1\\ (p-1)(q-1)(pq-p-q+5), & \text{if } \Delta_p=\Delta_q=1\\ (p-1)(q-1)(pq+p-q+1), & \text{if } \Delta_p=1,\Delta_q=-1\\ (p-1)(q-1)(pq-p+q+1), & \text{if } \Delta_p=-1,\Delta_q=1\\ (p-1)(q-1)(pq-p+3), & \text{if } \Delta_p=0,\Delta_q=1\\ (p-1)(q-1)(pq-q+1), & \text{if } \Delta_p=0,\Delta_q=-1\\ (p-1)(q-1)(pq-q+3), & \text{if } \Delta_p=1,\Delta_q=0\\ (p-1)(q-1)(pq+q+1), & \text{if } \Delta_p=-1,\Delta_q=0\\ (p-1)(q-1)(pq+2), & \text{if } \Delta_p=0,\Delta_q=0\end{cases}$$

Proof. By Lemma 1, $b\in\mathbb{Z}_{N,P}-\mathbb{Z}^*_{N,P}$ iff

$$|M_b|\equiv 0 \bmod p \text{ or } M_b\equiv 0 \bmod q$$

We have

$$\begin{aligned}-M_b &\equiv b_2^2-a_1b_1b_2+a_2b_1^2\\ &\equiv (b_2-\tfrac{N+1}{2}a_1b_1)^2-(\tfrac{N+1}{2}a_1^2b_1)^2+a_2b_1^2\\ &\equiv (b_2-\tfrac{N+1}{2}a_1b_1)^2-b_1^2(\tfrac{(N+1)^2}{4}a_1^2-a_2) \bmod N\end{aligned}$$

Thus we need look at the following equations

$$(b_2-\frac{N+1}{2}a_1b_1)^2\equiv b_1^2(\frac{(N+1)^2}{4}a_1^2-a_2) \bmod p \tag{3}$$

$$(b_2-\frac{N+1}{2}a_1b_1)^2\equiv b_1^2(\frac{(N+1)^2}{4}a_1^2-a_2) \bmod q \tag{4}$$

Case 1. If $b_1\equiv 0 \bmod p$, then (3) holds iff $b_2\equiv 0 \bmod p$, and if $b_1\equiv 0 \bmod q$, then (4) holds iff $b_2\equiv 0 \bmod q$.

Case 2. $b_1\not\equiv 0 \bmod p$. Then for fixed $b_1 \bmod p$, there are $0,1$, or 2 solutions $b_2 \bmod p$ for (3) iff

$$\Delta_p=-1,0,\text{ or }1$$

When $\Delta_p=0$, the solution is

$$b_2\equiv\frac{N+1}{2}a_1b_1 \bmod p \tag{5}$$

When $\Delta_1=1$, there is an $h\not\equiv 0 \bmod p$ such that

$$(b_2-\frac{N+1}{2}a_1)^2\equiv\frac{(N+1)^2}{4}a_1^2-a_2\equiv h^2 \bmod p$$

Thus

$$(b_2 - \frac{N+1}{2}a_1b_1)^2 \equiv b_1^2(\frac{(N+1)^2}{4}a_1^2 - a_2) \equiv (b_1h)^2 \bmod p.$$

Hence

$$b_2 - \frac{N+1}{2}a_1b_1 \equiv \pm b_1h \bmod p$$

i.e.

$$b_2 \equiv b_1(\frac{N+1}{2}a_1 \pm h) \bmod p \qquad (6)$$

Similarly, when $\Delta_q = 0$, the solution of (4) is

$$b_2 \equiv \frac{N+1}{2}a_1b_1 \mod q \qquad (7)$$

When $\Delta_q = -1$, (4) has no solution, and when $\Delta_q = 1$, there is a $k \not\equiv 0 \bmod q$ such that the solutions of (4) are

$$b_2 \equiv b_1(\frac{N+1}{2}a_1 \pm k) \bmod q \qquad (8)$$

Now according to the values of Δ_p and Δ_q, we need to treat 9 cases.

Case (-1,-1): $\Delta_p = \Delta_q = -1$.
In this case, (3) and (4) have no solutions, so $b \in \mathbb{Z}_{N,P} - \mathbb{Z}^*_{N,P}$ iff

$$b_1 \equiv b_2 \equiv 0 \bmod p \qquad (9)$$

or

$$b_1 \equiv b_2 \equiv 0 \bmod q \qquad (10)$$

The number of the pairs $(b_1, b_2) \bmod N$ satisfying (9) is q^2, and the number of those satisfying (10) is p^2. By Chinese Remainder Theorem, the number of the pairs $(b_1, b_2) \bmod N$ satisfying both (9) and (10) is 1. So the total number of the elements in $\mathbb{Z}_{N,P} - \mathbb{Z}^*_{N,P}$ is $p^2 + q^2 - 1$.

Therefore, $\Delta_p = \Delta_q = -1$ implies

$$\phi(N, P) = p^2q^2 - p^2 - q^2 + 1 = (p^2 - 1)(q^2 - 1)$$

Case (0,0): $\Delta_p = \Delta_q = 0$.
In this case, the number of the solutions $(b_1, b_2) \bmod N$ with $b_1 \not\equiv 0 \mod p, b_2 \not\equiv 0 \bmod q$ of (5) and (7) are $(p-1)(q-1)q$ and $(p-1)(q-1)p$, since the number of $b_1 \bmod N$ satisfying $b_1 \not\equiv 0 \bmod p$ and $b_2 \not\equiv 0 \bmod q$ is $(p-1)(q-1)$. For any such $b_1 \bmod N$, by Chinese Remainder Theorem, there is just one $b_2 \mod N$ satisfying both (5) and (7). Thus the total number of the elements in $\mathbb{Z}_{N,P} - \mathbb{Z}^*_{N,P}$ is

$$p^2 + q^2 - 1 + (p-1)(q-1)q + (p-1)(q-1)p - (p-1)(q-1)$$

Hence

$$\phi(N,P) = (p-1)(q-1)(pq+2)$$

Case (1,1): $\Delta_p = \Delta_q = 1$. Then the number of the solutions $(b_1, b_2) \bmod N$ with $b_1 \not\equiv 0 \bmod p$ and $b_1 \not\equiv 0 \bmod q$ of (6) and (8) are $2(p-1)(q-1)q$ and $2(p-1)(q-1)p$ and the number of the common ones for (6) and (8) is $4(p-1)(q-1)$. Thus

$$\phi(N,P) = (p-1)(q-1)(pq-p-q+5)$$

Case (1,-1). For $b_1 \bmod N$ with $b_1 \not\equiv 0 \bmod p$ and $b_1 \not\equiv 0 \bmod q$, (6) has $2(p-1)(q-1)q$ solutions $(b_1, b_2) \bmod N$, and (4) has no solution. Thus

$$\phi(N,P) = (p-1)(q-1)(pq+p-q+1)$$

Symmetrically, we have the result for

Case (-1,1): $\phi(N,P) = (p-1)(q-1)(pq-p+q+1)$.

Case (0,1). For $b_1 \bmod N$ with $b_1 \not\equiv 0 \bmod p$ and $b_1 \not\equiv 0 \bmod q$, (5) has $(p-1)(q-1)q$ solutions $(b_1, b_2) \bmod N$, and (8) has $2(p-1)(q-1)p$ solutions $(b_1, b_2) \bmod N$ with $2(p-1)(q-1)$ solutions in common with (5)'s. Thus

$$\phi(N,P) = (p-1)(q-1)(pq-p+3)$$

Symmetrically, we have the result for

Case (1,0): $\phi(N,P) = (p-1)(q-1)(pq-q+3)$.

Case (0,-1). The same argument as above leads to

$$\phi(N,P) = (p-1)(q-1)(pq+p+1)$$

Case (-1,0). $\phi(N,P) = (p-1)(q-1)(pq+q+1)$.
The proof is complete.

In Prop. 1, in the case $\Delta_p = \Delta_q = -1$, we see that $b \in \mathbb{Z}^*_{N,P}$ iff $(b_1, b_2) \not\equiv (0,0) \bmod p$, and $(b_1, b_2) \not\equiv (0,0) \bmod q$; and $\Delta_p = \Delta_q = -1$ is equivalent to $x^2 + a_1 x + a_2$ being irreducible both over F_p and F_q.

Since then $F_{p^2} = \mathbb{Z}_N[x]/P \bmod p$, and $F_{q^2} = \mathbb{Z}_N[x]/P \bmod q$, we see that $b \in \mathbb{Z}^*_{N,P}$ iff $b \bmod p \in F^*_{p^2}$ and $b \bmod q \in F^*_{q^2}$. Thus there is a group isomorphism:

$$\mathbb{Z}^*_{N,P} \mapsto F^*_{p^2} \times F^*_{q^2}$$

This deduction can be generalized to the following:

Proposition 2. Let $N = pq$ with p and q odd primes, and $P = x^m + a_1 x^{m-1} + \cdots + a_m$ be irreducible both over F_p and F_q. Then the map $\mathbb{Z}_{N,P} \longrightarrow F_{p^m} \times F_{q^m}$ given by

$$b = b_1 x^{m-1} + \cdots + b_m \mapsto (b \bmod p, b \bmod q)$$

induces a group isomorphism

$$\mathbb{Z}^*_{N,P} \mapsto F^*_{p^m} \times F^*_{q^m}$$

and

$$\phi(N,P) = (p^m - 1)(q^m - 1)$$

Proof. By Lemma 1, $b \in \mathbb{Z}^*_{N,P}$ iff $|M_b| \in \mathbb{Z}^*_N$. And $|M_b| \in \mathbb{Z}^*_N$ iff $|M_b| \bmod p \not\equiv 0$ and $|M_b| \bmod q \not\equiv 0$, i.e. $b \bmod p \in F^*_{p^m}$ and $b \bmod q \in F^*_{q^m}$. Moreover, by Chinese Remainder Theorem, it is easily seen that the map $b \to (b \bmod p, b \bmod q)$ is a bijection between $\mathbb{Z}_{N,P}$ and $F_{p^m} \times F_{q^m}$. Hence $\mathbb{Z}^*_{N,P} \to F^*_{p^m} \times F^*_{q^m}$ is an isomorphism and $\phi(N,P) = (p^m - 1)(q^m - 1)$. The proof is complete.

3 Correctness of the systems

As we state in the introduction, for $N = pq$ with p and q big different primes, $P = x^m + a_1x^{m-1} + \cdots + a_m$ being special to N, M being any common multiple of $p^m - 1$ and $q^m - 1$, $e \in \{2, 3, \cdots, M-1\}$ with $\gcd(e, M) = 1$, $d \in \{2, \cdots, M-2\}$ with

$$ed \equiv 1 \bmod M$$

the public key K of the system is (N, P, e), and the secret key is d . For any $y \in \mathbb{Z}_{N,P}$, if $y \in \mathbb{Z}^*_{N,P}$, then

$$y^{ed} \equiv y \bmod P$$

To ensure the correctness of the system, we have to prove that the above formula is also true for any $y \in \mathbb{Z}_{N,P} - \mathbb{Z}^*_{N,P}$.

Let $y \neq 0$ be so. We may assume $y \bmod p = 0 \in F_{p^m}$. Then $y \bmod q \neq 0$ as an element of F_{q^m}.

Since the number of $F^*_{q^m}$ is $q^m - 1$, we have

$$y^{q^m-1} = 1 \bmod P \,\text{on}\, F_q$$

Let $ed = 1 + kM$, where $k \in Z$, and $M' = M/(q^m - 1)$. We have then

$$y^{k(q^m-1)M'} \equiv 1 \bmod P \,\text{on}\, F_q$$

i.e. if regarding $y = y_1x^{m-1} + \cdots + y_m \in \mathbb{Z}[x]$, and $y^{kM} \in \mathbb{Z}[x]$ is written as $z_1x^{m-1} + \cdots + z_m + Q(x)P(x)$, then

$$z_1x^{m-1} + \cdots + z_m = 1 + q(u_1x^{m-1} + \cdots + u_m)$$

for some $u_i \in \mathbb{Z}, i = 1, \cdots, m$. According to the assumption on y, $y = p(v_1x^{m-1} + \cdots + v_m)$ for some $v_i \in \mathbb{Z}, i = 1, \cdots, m$. Thus

$$\begin{aligned} y^{kM+1} = y + \quad & pq(u_1x^{m-1} + \cdots + u_m)(v_1x^{m-1} + \cdots + v_m) + \\ & p(v_1x^{m-1} + \cdots + v_m)Q(x)P(x) \end{aligned}$$

So $y^{kM+1} = y^{ed} = y$ in $\mathbb{Z}_{N,P}$, and any message $y \in \mathbb{Z}_{N,P}$ is recovered by y^{ed}.

Notice that if one of the Δ_p and $\Delta_q$vanishes, say $\Delta_p = 0$, then $P \equiv x^2+a_1x+a_2 \equiv (x+a)^2 \bmod p$ for some $a \in \mathbb{Z}$. Thus for

$$y = x + a \in \mathbb{Z}_{N,P}$$

$y^{\phi(N,P)} = (x+a)^2(x+a)^{\phi(N,P)/2} \equiv 0 \bmod P$ and p, since $\phi(N,P)/2 \in \mathbb{Z}$. Now if $ed = 1 + k\phi(N,P)$ with $0 \neq k \in \mathbb{Z}$, we have

$$y^{ed} \equiv 0 \bmod P \text{ and } p$$

So $y^{ed} \neq y$ in $\mathbb{Z}_{N,P}$, since $y \not\equiv 0 \bmod P$ and p. Thus we have the following

Question. For $P = x^2 + a_1x + a_2$ not special to $N = pq$ with $|\Delta_p| = |\Delta_q| = 1, ed \equiv 1 \bmod \phi(N,P)$, is $y^{ed} = y$ for any $y \in \mathbb{Z}_{N,P}$?

Acknowledgement The author thanks Mingsheng Wang, Dingkang Wang, Dongdai Lin and Fusheng Ren for helpful discussions.

References

[1] R.L.Rivest, A.Shamir and M.Adleman, A method for obtaining digital signature and public-key cryptosystems, Communication of the ACM, 21 (2) (1978),120-126

[2] Joachm Von zur gathen and Jurgen Gerhard, Modern Computer Algebra, Cambrige University Press,1999

Author's Address:
Key Laboratory of mathematics Mechanization
Academy of Mathematics and Systems Science,
Chinese Academy of Sciences, Beijing 100080
Email: libh@amss.ac.cn