Some Remarks on Multi-prime RSA

Raluca Andreea Diaconu, Manfred Kudlek
email: raluca.diaconu@info.uaic.ro,kudlek@informatik.uni-hamburg.de

Abstract

We present the mathematical background for a general multi-prime cryptosystem, showing that such exists if and only if the module m is a product of simple primes, i.e. is square-free. The group of keys is commutative and has the cardinality $\varphi(\varphi(m))$.

1 Introduction

In the history of cryptology several methods of encryption using mathematical operations on $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ with $m \in \mathbb{N}$, $m > 1$ have been introduced. If not mentioned explicitly, in an expression $a \pmod m$ it is understood that $0 \leqslant a < m$. For more details from cryptology see e.g. [5, 6], and from number theory e.g. [1, 3, 4].

The first method, usually named after **Caesar**, use *addition*. In this case encryption is defined by $y \equiv f_e(x) \equiv x + e \pmod m$, e being the key, and decryption then is given by $d \equiv m - e \pmod m$ such that $f_e^{-1} = f_d$ and $f_d(y) \equiv f_d(f_e(x)) \equiv x + e + d = x \pmod m$. Thus the group of encryption functions (keys) is $\mathbb{Z}_m$ and $|\mathbb{Z}_m| = m$.

The second operation used is *multiplication*. Encryption is defined by $f_e(x) = x \cdot e$. In this case, however, not for every f_e there exists an inverse. That exists if and only if $(e, m) = 1$, i.e. e and m are prime to each other. The group of encryption functions (keys) then is given by $\{z \in \mathbb{Z}_m \mid (z, m) = 1\}$, and it has the cardinality $\varphi(m)$ where φ denotes the **Euler** totient function. The inverse function $f_e^{-1} = f_d$ is given by d with $e \cdot d \equiv 1 \pmod m$.

The next natural operation would be *exponentiation*, such that encryption is defined by $f_e(x) \equiv x^e \pmod m$. As in the case of multiplication, the inverse does not exist for every e. One has

$f_e(xy) \equiv (xy)^e \equiv x^e y^e \equiv f_e(x) f_e(y) \pmod{m}$
$f_d(f_e(x)) \equiv f_d(x^e) \equiv x^{de} \equiv x^{ed} \equiv f_e(x^d) \equiv f_e(f_d(x)) \pmod{m}$.
Therefore $f_e f_d = f_d f_e = f_{ed} = f_{de}$, and therefore also $f_e(f_d f_c) = (f_e f_d) f_c$.
Furthermore, $f_0(x) = x^0 = 1$, and $f_1(x) = x^1 \equiv x \pmod{m}$.
Thus the set of functions f_e with $e \neq 0$ is a commutative monoid.

The simplest case with exponentiation is $m = p_1$, a prime number. This, in some sense similar to the cryptosystems with addition or multiplication, cannot be used as a public key cryptosystem.

The most famous encryption method, **RSA**, introduced in 1977 by **Ronald Rivest, Adi Shamir,** and **Leonard Adleman**, applies exponentiation for $m = p_1 \cdot p_2$ where p_1 and p_2 are two prime numbers, giving a public key cryptosystem.

It is the aim of this article to investigate the set of invertible encryption functions for every $m > 1$.

First we show a simple lemma for non-existence of an inverse of f_e. Let $e > 1$.

Lemma 1: If $e \equiv 2 \pmod{m}$ then $\neg\exists f_e^{-1}$.
Proof: $1 \equiv 1^2 \equiv (m-1)^2 \pmod{m}$. □

For the general case of the module m we represent $\mathbb{Z}_m$ as a Cartesian product (see e.g. [3]).
For this let

$$m = \prod_{i=1}^{k} p_i^{\alpha_i}$$

Then

$$\mathbb{Z}_m \simeq \bigtimes_{i=1}^{k} \mathbb{Z}_{p_i^{\alpha_i}}$$

and the Euler function is given by

$$\varphi(m) = \prod_{i=1}^{k} (p^{\alpha_i} - p^{\alpha_i - 1}) = \prod_{i=1}^{k} p_i^{\alpha_i - 1}(p_i - 1) \ .$$

Elements of $\mathbb{Z}_m$ then are $(x_1, \cdots, x_k)$, with $x_i \in \mathbb{Z}_{p_i^{\alpha_i}}$ and $x \equiv x_i \pmod{p_i^{\alpha_i}}$.

Then x is given as the unique solution of the system $x \equiv x_i \pmod{p_i^{\alpha_i}}$ with $0 \leqslant x < m$ by the Chinese remainder theorem.

The operations are given by

$(x_1, \cdots, x_k) + (y_1, \cdots, y_k) \equiv (x_1 + y_1, \cdots, x_k + y_k) \pmod{(p_1^{\alpha_1}, \cdots, p_k^{\alpha_k})}$,

$(x_1, \cdots, x_k) \cdot (y_1, \cdots, y_k) \equiv (x_1 \cdot y_1, \cdots, x_k \cdot y_k) \pmod{(p_1^{\alpha_1}, \cdots, p_k^{\alpha_k})}$,

as well as

$(x_1, \cdots, x_k)^e \equiv (x_1^e, \cdots, x_k^e) \pmod{(p_1^{\alpha_1}, \cdots, p_k^{\alpha_k})}$.

Zero is $(0, \cdots 0)$, and unit $(1, \cdots, 1)$.

Finally, x^{-1} exists if and only if all x_i^{-1} exist, and then x^{-1} is represented by $(x_1^{-1}, \cdots, x_k^{-1})$.

Since this representation is rather different from the classical one, we give an example for $m = 2 \cdot 3 \cdot 5$.

0	(0,0,0)	10	(0,1,0)	20	(0,2,0)
1	(1,1,1)	11	(1,2,1)	21	(1,0,1)
2	(0,2,2)	12	(0,0,2)	22	(0,1,2)
3	(1,0,3)	13	(1,1,3)	23	(1,2,3)
4	(0,1,4)	14	(0,2,4)	24	(0,0,4)
5	(1,2,0)	15	(1,0,0)	25	(1,1,0)
6	(0,0,1)	16	(0,1,1)	26	(0,2,1)
7	(1,1,2)	17	(1,2,2)	27	(1,0,2)
8	(0,2,3)	18	(0,0,3)	28	(0,1,3)
9	(1,0,4)	19	(1,1,4)	29	(1,2,4)

2 The General Case

In this section we exhibit the conditions for the existence of the inverse function f_e.

The first theorem states that the inverse f_e^{-1} does not exist if m contains a square.

Theorem 1: If $\exists i \ : \ \alpha_i \geqslant 2$ then $\neg \exists f_e^{-1}$ for $e > 1$.

Proof: For $e \equiv 0 \pmod 2$ this follows immediately from

$1 = 1^2 \equiv (m-1)^2$.

Thus assume $e \equiv 1 \pmod 2$. It suffices to show the claim for one p only.

Now $p^{(\alpha-1)e} = p^{\alpha} p^{\alpha(e-1)-e}$.

1) $p > 2, m = p^\alpha$:
Since $\alpha(e-1) - e \geqslant 2(e-1) - e = e - 2 \geqslant 0$ for $\alpha \geqslant 2$ and $e \geqslant 2$
it follows that $p^{(\alpha-1)e} \equiv 0 \pmod{p^\alpha}$ if $\alpha \geqslant 2, e \geqslant 2$
and also $(2p^{\alpha-1})^e = 2^e p^{(\alpha-1)e} \equiv 0 \pmod{p^\alpha}$.
Note that $0 < p^{\alpha-1} < 2p^{\alpha-1} < p^\alpha$.

2) $m = 2^\alpha, \alpha \geqslant 3$:
$2^{(\alpha-2)e} = 2^\alpha 2^{\alpha(e-1)-2e} \equiv 0 \pmod{2^\alpha}$ if $e \geqslant 3$
$2^{(\alpha-1)e} = 2^\alpha 2^{\alpha(e-1)-e} \equiv 0 \pmod{2^\alpha}$ if $e \geqslant 2$.
Note that $0 < 2^{\alpha-2} < 2^{\alpha-1} < 2^\alpha$.

3) $m = 4p, p > 2$:
For this use induction over e
$(3p+1)^2 - (p+1)^2 = 8p^2 + 4p^2 \equiv 0 \pmod{4p}$
$(3p+1)^e - (p+1)^e \equiv 0 \pmod{4p}$
$(3p+1)^{e+1} - (p+1)^{e+1} = (3p+1)(3p+1)^e - (p+1)(p+1)^e$
$= 2p(3p+1)^e + (p+1)((3p+1)^e - (p+1)^e) \equiv 0 \pmod{4p}$
since $(3p+1)^e \equiv 0 \pmod{2}$.
Note that $0 < p+1 < 3p+1 < 4p$.

4) $m = 4$:
Trivial.

□

Thus there exist an inverse f_e^{-1} only if m has no square factor.
To proof the main theorem we need a generalization of the Euler theorem.

Theorem 2: If

$$m = \prod_{i=1}^{k} p_i$$

then $\forall x \in \mathbb{Z}_m \ : \ x^{n\varphi(m)+1} \equiv x \pmod{m}, n \in \mathbb{N}$.

Proof: Consider $x = (x_1, \cdots, x_k)$. Then $x_i^{\varphi(p_i)} \equiv 1 \pmod{p_i}$ for $x_i \neq 0_i$, and therefore, since $\varphi(p_i) | \varphi(m)$, $x_i^{\varphi(p_i)} \equiv 1_i \pmod{p_i}$ for $x_i \neq 0_i$. This implies $x_i^{\varphi(m)+1} \equiv x_i \pmod{p_i}$ for $x_i \neq 0_i$.

Now also $0_i^{\varphi(m)+1} \equiv 0_i \pmod{p_i}$. From this follows
$x^{\varphi(m)+1} = (x_1^{\varphi(m)+1}, \cdots, x_k^{\varphi(m)+1}) \equiv x = (x_1, \cdots, x_k) \pmod{(p_1, \cdots, p_k)}$.

Since also $x_i^{n\varphi(p_i)} \equiv 1_i \pmod{p_i}$ for $x_i \neq 0_i$ and $0_i^{n\varphi(p_i)} \equiv 0_i \pmod{p_i}$ it follows also $x^{n\varphi(m)+1} \equiv x \pmod{m}$.

□

Thus there are at most $\varphi(m)$ different functions f_e.

Theorem 2 does not hold in the general case, i.e. take $m = 18$ with $\varphi(m) = 6$, giving $3, 3^2 = 9, 3^3 = 9, \cdots$.

In the next theorem we give the exact structure of the group of invertible functions in the general case.

Theorem 3: If

$$m = \prod_{i=1}^{k} p_i$$

then $(e, \varphi(m)) = 1 \Leftrightarrow \exists f_e^{-1}$.

Proof:

$(\Rightarrow)$ $(e, \varphi(m)) = 1 \Rightarrow \exists d = e^{-1} \ : \ ed \equiv 1 \pmod{\varphi(m)}$.

$\Rightarrow \forall x \ : \ x^{ed} \equiv x^{n\varphi(m)+1} \pmod{m} \equiv x \pmod{m}$

$\Rightarrow f_e^{-1} = f_d$.

$(\Leftarrow)$ If $\exists f_e^{-1} = f_d$ then $\forall x \ : \ x^{ed} \equiv x \pmod{m}$. It can be assumed that $d, e > 1$ and d, e odd.

Let $\lambda(\varphi(m)) = [(\varphi(p_1), \cdots, \varphi(p_k)]$ (least common multiple). Consider primitive roots $x_i \in \mathbb{Z}_{p_i}, 1 \leqslant i \leqslant k$. Then $o(x_i) = \varphi(p_i)$, and it follows $x_i^{\varphi(p_i)} \equiv 1 \pmod{p_i}$. If $x = (x_1, \cdots, x_k)$ then

$x^{\lambda(\varphi(m))} = (x_1^{\lambda(\varphi(m))}, \cdots, x_k^{\lambda(\varphi(m))}) \equiv (1, \cdots, 1) \pmod{(p_1, \cdots, p_k)}$

$\equiv 1 \pmod{m}$.

$\lambda(\varphi(m))$ is the smallest exponent for x with this property since otherwise there would exist a j with $\varphi(p_j)$ not dividing an exponent $c < \lambda(\varphi(m))$ resulting in $x^c \not\equiv 1 \pmod{m}$.

Furthermore, for all $y \in \mathbb{Z}_m$ follows $o(y) | \lambda(\varphi(m))$ since for $y = (y_1, \cdots, y_k)$ holds $o(y_j) | \varphi(p_j)$ and therefore $[(o(y_1), \cdots, o(y_k))] | \lambda(\varphi(m))$.

Now $\exists x^{-1} = (x_1^{-1}, \cdots, x_k^{-1})$, and therefore $x^{ed-1} \equiv 1 \pmod{m}$.

Thus $\lambda(\varphi(m)) | (ed - 1)$ implying $(ed, \lambda(\varphi(m))) = 1$.

If $(e, \varphi(m)) > 1$ then also $(e, \lambda(\varphi(m)) > 1$ and thus $(ed, \lambda(\varphi(m)) > 1$, a contradiction.

□

Thus the group of invertible functions consists of exactly $\varphi(\varphi(m))$ elements, and is commutative.

Note the relation to Carmichael's theorem stating that

$x^{\psi(n)} \equiv 1 \pmod{n}$ if $(x,n) = 1$, where
$\psi(2^k) = 2^{k-1}$ if $k \leqslant 2$,
$\psi(2^k) = 2^{k-2}$ if $k > 2$,
$\psi(p^k) = p^{k-1}(p-1)$ if $p > 2$ prime,
$\psi(p_1^{k_1} \cdots p_m^{k_m}) = [\psi(p_1^{k_1}), \cdots, \psi(p_m^{k_m})]$.

For given $\varphi(\varphi(m))$ the group of invertible functions is not unique as can be seen from the following two examples.

a) $m = 3 \cdot 5$ giving $\varphi(15) = 8$ and $\varphi(\varphi(15)) = 4$ and the group

	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

having no generator and being a direct product of 2 groups of order 2.

b) $m = 2 \cdot 11$ giving $\varphi(22) = 10$ and $\varphi(\varphi(22)) = 4$ and the group

	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

having generators 3 and 7, and therefore not being isomorphic to the first group.

Consider again

$$m = \prod_{i=1}^{k} p_i \ ,$$

assume $(e, \varphi(m)) = 1$. Let $x \in \mathbb{Z}_m$, define $x_i \in \mathbb{Z}_{p_i}$ by $x \equiv x_i \pmod{p_i}$. Then $x^e \equiv x_i^e \pmod{p_i}$. Similarly, define $e_i \in \mathbb{Z}_{p_i - 1}$ by $e \equiv e_i \pmod{p_i - 1}$. Then $x_i^e \equiv x_i^{e_i} \pmod{p_i}$ by Euler's theorem. Note that this holds also for $x_i = p_i \equiv 0 \pmod{p_i}$. Therefore, $x^e \equiv x_i^{e_i} \pmod{p_i}$.

Let $y = x^e \pmod{m}$ and $ed \equiv 1 \pmod{\varphi(m)}$. In the same way as above define y_i by $y \equiv y_i \pmod{p_i}$, and d_i by $d \equiv d_i \pmod{p_i - 1}$. Then

$e_i d_i \equiv e_i d \equiv ed \equiv 1 \pmod{p_i - 1}$. Thus $y_i^{d_i} \equiv x_i^{e_i d_i} \equiv x_i \pmod{p_i - 1}$.

A multiprime cryptosystem applying the results given above has been introduced in [2].

References

[1] Tom M. Apostol: *Introduction to Analytic Number Theory.* Undergraduate Texts in Mathematics, Springer, 1976.

[2] Thomas Collins, Dale Hopkins, Susan Langford, Michael Sabin: *Multiprime RSA Public Key Cryptosystem.* United States Patent 7231040, 1998.

[3] Kenneth Ireland, Michael Rosen: *A Classical Introduction to Modern Number Theory.* Springer Graduate Texts in Mathematics 84, 1972, 1982.

[4] Gareth A. Jones, J. mary Jones: *Elementary Number Theory.* Springer, 2006.

[5] Douglas R. Stinson: *Cryptography, Theory and Practice.* Chapman & Hall, 2002.

[6] Samuel S. Wagstaff: *Cryptanalysis of Number theoretic Ciphers.* Chapman & Hall/CRC, 2003.