The Cubic Public-Key Transformations

**Abstract**

This paper presents the cubic public key transformation with modulo primes and composite numbers where the mapping is not one-to-one.

**Introduction**

The cubic transformation is used for public key applications and digital signatures, in which message m is encrypted to cipher using c = m3 mod n, n = p\*q and p and q are primes, and Euler totient function ϕ(n) is divisible by 3 but not by 9. This transformation is more efficient than the square transformation proposed by Michael Rabin. In his article he had discounted the cubic transformations, implicitly taken n to be divisible by 9. This cubic transformation deals with the case that Rabin overlooked.

**The Properties of the cubic transformation**

We first consider cubic modulo mapping of a prime number. For cubic transformation c=m3 mod p, three different values of message m would give the same cipher c, where p = 3k+1 is prime, and p = 3 mod 4.

The cube roots of 1 are 1, α and α2 and they are calculated by solving the equation:

α3 – 1 = 0

(α - 1)(α2 + α + 1) = 0

The roots obtained from the above equation are:

α = 1

α 1= (-1 + (p - 3))

α 2= (-1 - (p - 3))

When Euler totient function ϕ(n) = (p - 1) is not divisible by 9, Bob finds one of its cubic roots by means of an inverse exponentiation operation:



**Problem 1**: Cubic Transformation Modulo of a Prime Number

Let Alice choose a prime number p = 727, where p = 3(242) + 1.

To compute α, we must find

x = (p-3)(p+1)/4 = 618

And where α1 = (-1+618+h\*p) = 672 and α2 = (-1-618+h\*p) = 54.

Chose α = α2 = 54.

Table 1. Communication between Alice & Bob

|  |  |
| --- | --- |
| Alice | Bob |
| 1. Let message m chosen by Alice = 4. 2. After computing m, mα, mα2 and arranging them in ascending order, Alice gets [4, 32, 216]. 3. The rank of the message m = 4 is 1, so the side information based on the message chosen is 1. 4. Alice sends c = m3 mod p = 64 mod 727 = 64 and also sends side information = 1 to Bob. | 1. By substituting i = 1, Bob finds out that a = (i\*p+2)/9 = 81 using the above equation. 2. Bob gets one of the cubic roots as   b1 = (ca) mod p = 4  and other roots as  b2 = (b1 \* α) mod p = 216  b3 = (b2 \* α) mod p = 32   1. Arranging them in ascending order Bob gets [4, 32, 216] and side information=1 lets him know that the message chosen by Alice was m = 4. |

Table 2. Mapping for p = 727, α = 54

|  |  |  |  |
| --- | --- | --- | --- |
| m | mα | mα2 | C |
| 1 | 54 | 8 | 1 |
| 2 | 108 | 16 | 8 |
| 4 | 216 | 32 | 64 |
| 8 | 432 | 64 | 512 |
| 9 | 486 | 72 | 2 |
| 16 | 245 | 144 | 16 |

**Cubic transformation modulo a composite number**

The composite number, n is chosen such that it is composed of two primes n = p\*q, where Euler totient function ϕ(n) = (p - 1) (q - 1) is divisible by 3 but not by 9.

Then the inverse exponentiation operation is calculated by:



**Problem 2**: Cubic Transformation Modulo of a Composite Number

Let Alice choose a composite number n = 533, where n = p\*q = 13\*41.

P = 13, q = 41 and ϕ = (p - 1) (q - 1) = 480.

The roots of p, αp = {3, 4} and for q, αq = {1}

|| q-1||p = q-1 mod p = 7 and ||p-1||q = p-1 mod q = 19.

Using the Chinese Remainder Theorem

α = [ αp x q x || q-1||p + αq X p x ||p-1||q] mod n

α1 = [3 x 41 x 7 + 1 x 13 x 19] mod 533 = 42

α2 = [4 x 41 x 7 + 1 x 13 x 19] mod 533 = 329

Chose α = α1 = 42.

|  |  |
| --- | --- |
| Alice | Bob |
| 1. Let message m chosen by Alice=4. 2. After computing m, mα, mα2 and arranging them in ascending order, Alice gets [4,127,168]. 3. The rank of the message m=4 is 1, so the side information based on the message chosen is 1. 4. Alice sends c=m3mod ϕ= 64 and also sends side information=1 to Bob. | 1. By substituting i=1, Bob finds out that a=(i\*2\*ϕ+3)/9=107 using the above equation. 2. Bob gets one of the cubic roots as   b1=(ca)mod ϕ=168  and other roots as  b2=(b1\*α) mod p=127  b3=(b2\*α)mod p=4   1. Arranging them in ascending order Bob gets [4,127,168] and side information=1 lets him know that the message chosen by Alice was m=4. |

**ϕ(n) is divisible by 9**

When ϕ(n) is divisible by 9, the 9 cubic roots of 1 can be obtained from the equation

α9 – 1 = 0

(α3 - 1) (α3 + 1) = 0

(α3 + 1) (α2 + α + 1) = 0

The message that Alice wants to send to Bob would be multiplied with nine roots of 1 and arranged in ascending order so that its position in the set of nine numbers could be find out. Alice sends c = m3 mod n along with the position of the number as side information.

Bob will obtain c. He will find the cube root of c, then find the multiple of that number with all the roots of 1, arrange them in the ascending order and the position sent as side information lets him know the message that was sent by Alice.

**Problem 3**: If ϕ(n) is divisible by 9.

Let Alice choose a composite number n = 511, where n = p\*q= 7\*73.

P = 7, q = 73 and ϕ = (p - 1) (q - 1) = 432.

The roots of p, αp = {1, 2, 4} and for q, αq = {1, 2, 3}.

|| q-1||p = q-1 mod p = 5 and ||p-1||q = p-1 mod q = 21.

Using the Chinese Remainder Theorem

α =[ αp x q x || q-1||p + αq X p x ||p-1||q] mod n

,we can find the 9 cube roots.

α1 = [1 x 73 x 5 + 1 x 7 x 21] mod 511 = 1

α1 = [2 x 73 x 5 + 1 x 7 x 21] mod 511 = 2

α1 = [4 x 73 x 5 + 1 x 7 x 21] mod 511 = 74

α1 = [1 x 73 x 5 + 2 x 7 x 21] mod 511 = 148

α1 = [2 x 73 x 5 + 2 x 7 x 21] mod 511 = 149

α1 = [4 x 73 x 5 + 2 x 7 x 21] mod 511 = 221

α1 = [1 x 73 x 5 + 3 x 7 x 21] mod 511 = 295

α1 = [2 x 73 x 5 + 3 x 7 x 21] mod 511 = 366

α1 = [4 x 73 x 5 + 3 x 7 x 21] mod 511 = 368

The 9 roots after arranging them in the ascending order : [1 2 74 148 149 221 295 366 368 ]

|  |  |
| --- | --- |
| Alice | Bob |
| 1. Let message m chosen by Alice = 24. 2. After computing the 9 roots, Alice multiplies the roots with m = 24 and obtains [24 48 97 145 194 243 437 486 510] 3. The rank of the message m = 24 is 1, so the side information based on the message chosen is 1. 4. Alice sends c = m3mod ϕ = 27 and also sends side information = 1 to Bob. | 1. Bob finds out the cube root of 27 by using CRT or some probabilistic algorithm. 2. Arranging them in ascending order Bob gets [24 48 97 145 194 243 437 486 510] and side information = 1 lets him know that the message chosen by Alice was m = 24. |

**References**

1. S. Kak, A cubic public-key transformation, Circuits, Systems and Signal Processing 26:

353-359, 2007.

1. M.O. Rabin, Digitalized signatures and public-key functions as intractable as factorization. Technical Report MIT/CCS/TR-212. January 1979.
2. R.L. Rivest, A. Shamir and L.Adleman, A method for obtaining digital signatures and

public-key cryptosystems. Comm. ACM 21: 128-138, 1978.