PROPERTIES OF THE EULER TOTIENT FUNCTION MODULO 24 AND SOME OF ITS CRYPTOGRAPHIC IMPLICATIONS

Raouf N. Gorgui-Naguib and Satnam S. Dlay

Cryptology Research Group
Department of Electrical and Electronic Engineering
University of Newcastle upon Tyne
Newcastle upon Tyne NE1 7RU, England

ABSTRACT

The work reported in this paper is directed towards the mathematical proof of the existence of a consistent structure for the Euler totient function $\phi(n)$ given n. This structure is extremely simple and follows from the exploitation of some of the very interesting properties relating to the integer 24 as demonstrated in the proofs. This result is of particular concern to cryptologists who are either attempting to break the RSA or ascertain its cryptographic viability. Furthermore, it is stipulated that the methods and properties relating to the integer 24, taken as a modulo, may have strong implications on the different attempts to solve the factorisation problem.

I . INTRODUCTION

Rivest et. al. [1] (RSA) have presented a method for public-key cryptosystems, whose security depends predominantly on being able to factorise large numbers. This has stimulated research on the factorisation problem which would ultimately threaten the security of the RSA and has resulted in numerous papers being published on this work, such as Williams' overview of factoring procedures [2]. However, the validity of the different cryptanalytic attacks of the RSA has always been contested [3,4] and a fast algorithm for factorising large numbers has not yet appeared.

This paper does not set out to break the RSA, but approaches the factorisation problem from an original viewpoint and consequently raises some doubts about its security. The approach taken is the development of a mathematical proof of

the existence of a structure for the Euler totient function $\phi(n)$ in terms of the argument n. This structure could enable the computation of the decryption key, which is secret in the RSA cryptosystem, from a knowledge of the encryption key and the parameter n which both reside in the public directory. The derivation of the structure for the Euler totient function and its interesting implications is based on the extremely simple, but powerful, number theoretical properties of the integer 24.

II . NUMBER THEORETIC PROPERTIES OF THE INTEGER 24

In this section, we prove the existence of some extremely interesting properties relating to the integer 24. The most important of these properties may be expressed in terms of the following theorem:

Theorem 1 *For any prime p, $p > 3$,*

$$p^2 \equiv 1 \pmod{24} \tag{1}$$

Proof The congruence given in (1) can be expressed in the form of the Diophantine equation:

$$p^2 - 1 = 24k \tag{2}$$

for a particular value of k.

Hence,

$$\begin{aligned}(p-1)(p+1) &= 24k \\ &= 4!k\end{aligned}$$

where "!" denotes the factorial operation. The proof for (1) then consists in proving that $(p-1)(p+1)$ is divisible by 4, 3 and 2.

Since p is a prime, then its negative and positive differences about 1 can be expressed in the form:

$$\begin{aligned}(p-1) &= 2m \\ (p+1) &= 2m+2\end{aligned}$$

where m is any positive integer.

Hence,

$$\begin{aligned}(p-1)(p+1) &= 2m(2m+2) \\ &= 4m(m+1)\end{aligned}$$

If m is even, then $m = 2m'$. Conversely, if it is odd then $(m+1) = 2m'$, so that the product $m(m+1)$ is always an even integer of the form $2m''$. Thus

$$(p-1)(p+1) = 4.2m''$$

which establishes the fact that 2 and 4 are indeed factors of $p^2 - 1$.

To prove that the last factor 3 is also a factor of $p^2 - 1$, we present the following development.

Any three consecutive numbers about p will be of the form

$$p-1, \quad p, \quad p+1$$

and since $3 \not| p$ (p is a prime), then,

$$\begin{array}{ll} \textit{either} & 3 \mid (p-1) \\ \textit{or} & 3 \mid (p+1) \end{array}$$

In either case, the product $(p-1)(p+1)$ will consist of a factor of 3. This completes the proof.

III . DEDUCTION OF A STRUCTURE FOR THE EULER TOTIENT FUNCTION - CRYPTANALYSIS OF THE RSA MODULO 24

In this section, we present a stepwise mathematical deduction of the Euler totient function, $\phi(n)$, from a knowledge of n. This deduction is based on the theorem reported in the previous section.

In the case of the RSA [1],

$$n = pq$$

where p and q are the two primes involved in the encryption process.

The security of the RSA is based on the fact that a knowledge of, both, n and the encryption key. e (chosen at random from the interval $[2, \phi(n) - 1]$ such that $\gcd(e, \phi(n)) = 1)$), does not allow the straightforward deduction of the decryption key, d, where d is the multiplicative inverse of e modulo $\phi(n)$:

$$ed \equiv 1 \pmod{\phi(n)}$$

since, due to the factorisation problem and the nature of p and q, it is impossible to compute the value of $\phi(n)$ given n.

For two primes p and q, such that $p, q > 3$:

$$p^2 \equiv 1 \pmod{24}$$
$$q^2 \equiv 1 \pmod{24}$$

Then, for $n = pq$,

$$n^2 = p^2q^2 \equiv 1 \pmod{24} \tag{3}$$

Also, since $\phi(p^i) = p^{i-1}(p-1)$, [5], then

$$\begin{aligned}\phi(p^2) &= p(p-1)\\ &= p^2 - p\end{aligned}$$

or,

$$\phi(p^2) \equiv 1 - p \pmod{24} \tag{4}$$

Consequently, since $\gcd(p^2, q^2) = 1$, then

$$\begin{aligned}\phi(n^2) &= \phi(p^2)\phi(q^2)\\ &\equiv (1-p)(1-q) \pmod{24}\\ &\equiv 1 + pq - (p+q) \pmod{24}\\ &\equiv 1 + n - (p+q) \pmod{24}\end{aligned} \tag{5}$$

However,

$$\begin{aligned}\phi(n) &= (p-1)(q-1)\\ &= 1 + n - (p+q)\end{aligned} \tag{6}$$

From (5) and (6) we can then establish that

$$\phi(n^2) \equiv \phi(n) \pmod{24} \tag{7}$$

Also, since $\phi(p^2) = p(p-1)$, then congruence (5) can be interpreted as follows:

$$\begin{aligned}\phi(n^2) &= \phi(p^2)\phi(q^2)\\ &= p(p-1)\, q(q-1)\\ &= pq(p-1)(q-1)\end{aligned}$$

Thus,

$$\phi(n^2) = n\phi(n) \tag{8}$$

On the other hand, congruence (7) may be written in its Diophantine equation form:

$$\phi(n^2) = 24x + \phi(n) \qquad ; x = 1, 2, ... \tag{9}$$

Now, equating the RHS of equations (8) and (9) yields

$$n\phi(n) = 24x + \phi(n)$$

Hence

$$\phi(n) = \frac{24x}{n-1} \qquad ; x = 1, 2, ... \tag{10}$$

Equation (10) shows that there exists a definite structure for the Euler totient function in terms of its argument. In what concerns the RSA, such a structure is of particular importance since, for decryption purposes, $\phi(n)$ is the crucial secret number in the system. The ability to compute $\phi(n)$ given n renders the system vulnerable to cryptanalytic attacks and, although the practical evaluation of the factor x may still be complicated, it is thought that, in theory at least, the existence of such a structure may lead the way towards developing a fast algorithm for the evaluation of $\phi(n)$. This is currently being investigated.

IV . FURTHER PROPERTIES MODULO 24 AND AN ALGORITHM FOR EVALUATING ϕ(n)

The primes p and q involved in the RSA can be shown to have specific properties in terms of the integer 24, namely,

Theorem 2

$$p + q \equiv 2i \pmod{24} \qquad ; i = 0, 1, ..., 11 \tag{11}$$

The proof of this theorem is rather simple and shall not be presented here.

Conjecture 1 *The residue of $n = pq$ is always 1 or an odd prime, taken modulo 24. In general, we can write*

$$n \equiv \wp \pmod{24} \tag{12}$$

where $\wp = 1$ or a prime $\in$ [3,23].

Conjecture 2 *The residue of x in equation (10) is always an even integer, modulo 24:*

$$x \equiv 2j \pmod{24} \tag{13}$$

where j is an even or odd integer.

The development of the following algorithm depends on the two conjectures given above. From (12) and (13), we can write

$$x - n \equiv 2j - \wp \pmod{24}$$

or, that

$$x \equiv n + 2j - \wp \pmod{24} \tag{14}$$

In congruence (14), n is given and $\wp$ can be simply evaluated. Hence, the only missing parameter is j. Consequently, from this congruence, we may write

$$x = 24y + (n + 2j - \wp) \tag{15}$$

for a particular value of y. Replacing x in equation (10) by its corresponding expression in (15), we obtain

$$\phi(n) = \frac{24[24y + (n + 2j - \wp)]}{n - 1}$$

$$= \frac{24(n - \wp) + 24(24y + 2j)}{n - 1}$$

However, $(24y + 2j)$ will always yield an even value which may be expressed as $2i$ for any integer i. Hence,

$$\phi(n) = \frac{24(n - \wp) + 24.2i}{n - 1}$$

$$= \frac{24(n - \wp) + 48i}{n - 1} \tag{16}$$

As a result, the following algorithm may be developed based on equation (16) which searches for possible values of $\phi(n)$:

Step 1: Compute $\wp = n \pmod{24}$
Step 2: $\phi(n)$ is $O(n - 1)$;
hence the numerator in equation (16) is $O((n - 1)^2$.
Set numerator$= (n - 1)^2$
Step 3: Calculate a starting value of i, such that
$i = \lfloor[(n - 1)^2 - 24(n - \wp)]/48\rfloor$
Step 4: Check if $(n - 1) \mid$ numerator in equation (16):
Yes $\rightarrow$ possible value for $\phi(n)$ obtained, then
check equation (16), else
No $\rightarrow$ decrement i, and
repeat Step 4.

The above algorithm is by no means optimal. It suffers from two drawbacks: first, the magnitude of $(n-1)^2$ and, second, decrementing i by 1 results in a slow process. It is thought that a better approach may be to test for values of x, directly, in equation (10). This is currently being investigated and attempts to increase the multiplier of x from 24 to other larger integers, while maintaining a constant structure for $\phi(n)$, are also being studied.

V . CONCLUSIONS

In this paper we have presented a stepwise mathematical deduction of the Euler totient function $\phi(n)$ from a knowledge of n. This deduction is based on some interesting number theoretic properties relating to the integer 24. These properties, together with their proofs were presented in detail. An algorithm for the final evaluation of $\phi(n)$ was also given. However, it must be stressed that the aim of the paper was mainly directed towards proving the existence of a consistent structure for $\phi(n)$ in terms of n and the integer 24. It is believed that it may also have strong implications on the different attempts to solve the factorisation problem.

VI . ACKNOWLEDGEMENTS

The authors are grateful to their colleagues and postgraduate students in the Cryptology Research Group of the Department of Electrical and Electronic Engineering, the University of Newcastle upon Tyne, for many interesting discussions and comments on this work. They are particularly indebted to Jalil Tabatabaian for providing the simple proof of Theorem 1.

References

[1] R.L. Rivest, A. Shamir and L. Adleman, "A Method for Obtaining Digital Signature and Public-Key Cryptosystems", Communications of the ACM, vol. 21, No. 2, Feb. 1978, pp. 120-126.

[2] H.C. Williams, "An Overview of Factoring", Proceedings of CRYPTO'83, pp. 71-80.

[3] R.L. Rivest, "Remarks on a Proposed Cryptanalytic Attack on the M.I.T. Public-Key Cryptosystem", Cryptologia, vol. 2, No. 1, Jan. 1978, pp. 62-65.

[4] *ibid*, "Critical Remarks on 'Critical Remarks on Some Public-Key Cryptosystems' by T. Herlestam", BIT, vol. 19, 1979, pp. 274-275.

[5] G.H. Hardy and E.M. Wright, *An Introduction to the Theory of Numbers*, Oxford University Press, 1981.