A NEW REPRESENTATION FOR SEMI-PRIMES

Recent years have seen a considerable rise in interest in factoring large semi-primes N=pq of hundred digit length or larger. If the factoring of N should ever become a simple and rapid process, then the whole concept of public keys in modern day cryptography would become obsolete and electronic transmission of secret messages would require a brand new approach to that used in RSA cryptology. We want here to give some more consideration to the properties of large semi-primes and thereby shed some new light on the use of semi-primes N in modern day cryptography.

Any large semi-prime N consists of two primes p and q which can always be arranged so that –

$$p<\mathrm{sqrt}(N)<q$$

This means that-

$$p = \alpha\sqrt{N} \qquad and \qquad q = (1/\alpha)\sqrt{N}$$

Here α is a non-integer used to measure the departure of p and q from the root of N. For example, if we take the semi-prime-

N=pq=36781 x 58771=216156151 then sqrt(N)=46493.61409…

so that-

α=p/sqrt(N)= 0.7910978898…

Hence if we know the value of both N and α, the values of p and q are uniquely determined. For, example if –

N=2738157881 and α=0.6595587231…

we get-

p=αsqrt(N)=34513 and q=(1/α)sqrt(N)=79337

These results suggest that α will typically be a non-integer slightly below one. It also suggests we can define a new quantity-

$$M = \frac{(p+q)}{2\sqrt{pq}} = \frac{(1+\alpha^2)}{2\alpha}$$

which can be solved for α to yield-

$$\alpha = M - \sqrt{M^2 - 1} \qquad and \qquad (\frac{1}{\alpha}) = M + \sqrt{M^2 - 1}$$

Note that M contains all the information about the prime components p and q of the semi-prime N but in a very disguised form which is much more difficult to factor than N=pq is in standard RSA cryptology. We came up with the number M by remembering how non-dimensional quantities such as $E/(mc^2)$, F/(ma) , and VD/ν are constructed.

The parameter M specifically contains the information of how far p and q are removed from the square-root of N. That is p=αsqrt(N) and q=(1/α)sqrt(N). However, unless information concerning N is also given there is no easy way to find p and q. If one wants to include information about N, this can be accomplished by defining a second parameter-

$$K = \frac{q-p}{2N} = \frac{(1-\alpha^2)}{2\alpha\sqrt{N}}$$

After a little mathematical manipulation, this last parameter K and the other parameter M lead to the results-

$$p = \frac{(1-\alpha^2)}{2K} = \frac{(1-\alpha M)}{K} = \frac{(1+M\sqrt{M^2-1}-M^2)}{K}$$

$$\sqrt{N} = \frac{(1+M\sqrt{M^2-1}-M^2)}{K(M-\sqrt{M^2-1})}$$

$$q = \frac{(1+M\sqrt{M-1}-M^2)}{K(M-\sqrt{M^2-1})^2}$$

We thus have the factors p and q and the value of the semi-prime in encoded form provided by just two parameters M and K.

Let us look at an example where one has-

M= 1.114274336… and K= $2.398325355 \times 10^{-5}$

This produces at once the result that p=12763 , q=32911, and N=420043093 when rounding things off to the nearest integer.

The present procedure for disguising p, q, and N works for any size semi-prime including those fifty to one hundred digit long Ns used in RSA cryptography. To encrypt such Ns one first generates two prime numbers by a procedure discussed in one of our earlier notes of combing products of irrational numbers such as ln(2), π, and exp(1). Here we find after a few minutes the fifty digit long primes-

p=23213404357363387236150345896006882480062932649067

and-

q=34509766067530130102032459040061606134055036821113

The corresponding semi-prime reads-

N=
801089154003595086850771904260898825347665205386392985820921184989047985564963433990166867685351571

A quick evaluation produces the parameters-

M=
1.01971722388846063415493818207816389929752338525597083746697572780419578290745593038538291…

and-

K=
705062704551112149542352033710342040529772269607195362721248501392880223404294619623831897 x 10^{-50} .

Sender A can now transmit these values as a public key to receiver B and any possible adversary C listening. However it will be only A and B who will understand how M and K have been generated. Both A and B will now know the value of the fifty digit long prime p if B uses the formula-

$$p = \frac{(1 + M\sqrt{M^2 - 1} - M^2)}{K}$$

Having found p the receiver B can now attach a message m to p and send the combination to A. Upon receipt, A can perform the operation (p+m)-p=m to recover the message. The main weakness of this public key procedure is that an adversary C might figure out the formulas for M and K being used. Without these formulas, the value of p will be essentially impossible to find. As further protection against adversaries, M and K should often be changed and the message m further encrypted before combining with p. The length of p and the message m should be of comparable length. Twitter followers will be familiar with creating short messages.

We finish by seeing what disguised message receiver B is sending A in response to the input-

$$M=1.1142744336.. \quad \text{and} \quad K=2.398325355 \times 10^{-5}$$

B figures out the corresponding p and sends the disguised message (p+m) back to A. The signal sent is-

$$m+p= 15121$$

When A receives this information he subtracts out the known p to get-

$$m=2358$$

That is, B has sent A the first four numbers of the familiar Fibonacci sequence.

December 1, 2015