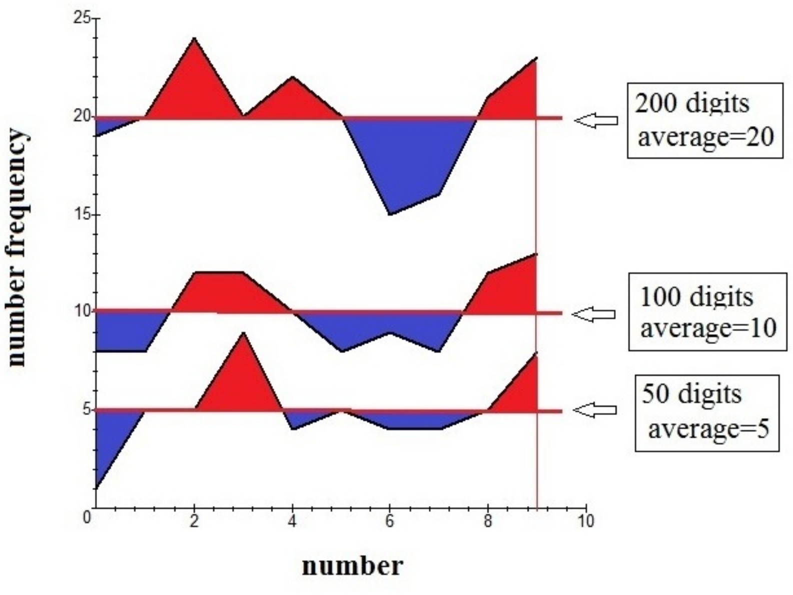
TRANSMITTING AND RECEIVING MESSAGES USING KNOWN RANDOM NUMBERS CREATED FROM IRRATIONALS

It is well known that standard modern day cryptography relies on the use of the product of two large prime numbers onto which are added messages readable only by a friendly receiver. The details of the procedure is rather complicated but is considered secure since it relies on the inability of any adversary to factor large semi-prime public keys in any reasonable amount of time using even the fastest supercomputers. We propose here a simpler alternate method for transmitting secret information using only the product of a message and a single random number N, not necessarily prime, constructed from products of well known irrational numbers. The basic idea behind the transmission scheme is that such numbers can be readily generated and are expressible in an extremely compressed form which acts as a password. Only the sender and a friendly receiver will be familiar with this password.

GENERATING RANDOM NUMBERS USING IRRATIONALS:

There are an infinite number of irrational numbers encountered in mathematics whose digits appear in an essentially random manner. Although their digit frequency 0 to 9 in any length interval L may not be exactly equal to L/10 for each of the possible ten digits , their average value will be equal to this amount. We demonstrate this behavior for the irrational number π in the following graph-

NUMBER FREQUENCY IN PI WHEN COUNTING THE FIRST 50, 100, AND 200 DIGITS



The graph clearly shows that the ten digits 0 through 9 are not equally distributed in the three chosen intervals L but their average still adds up L/10. So we may still refer to the digits in π as appearing randomly although the actual number frequency lies above the average for 3 and 9 and below the average for 0 and 6. The number frequency is also seen to vary with the digit length being examined, although the average remains L/10 . Such number frequency variations do not preclude the use of N as a carrier for sending secure messages M over the airwaves in the form of NM. No one, not familiar with the N being used, will be able to factor NM in any reasonable amount of time.

To generate some product forms involving irrationals we start by writing down some of the best known irrationals to fifty place accuracy-

π= 3.1415926535897932384626433832795028841971693993751

exp(1)= 2.7182818284590452353602874713526624977572470937000

ln(2)= 0.69314718055994530941723212145817656807550013436026

φ=[1+sqrt(5)]/2= 1.6180339887498948482045868343656381177203091798058

γ=0.57721566490153286060651209008240243104215933593992

We can assign the temporary (and readily changeable) code names P, E, L, F, and G to these. Also we can add an infinite number of other irrational numbers such as sqrt(2) and the cube root of 13 to this collection. In addition we can use symbols such as S standing for taking a square root of all terms following it and C for taking a cube root of the combination of symbols following it.

If we now take the products of several of these irrationals, a large random number product N can be created which is expressible in compact form using only a few symbols. As an example , consider the fifty place approximation to-

SEPG=sqrt[exp(1)*Pi*gamma]

= 2.2201955696341027271287691074303934017355053109854

Placing a number 5 in front of the expression means that we are referring to starting the irrational number 5 places to the right of its decimal point. The resultant irrational forty-five digit long number reads–

N=5SEPG= 955696341027271287691074303934017355053109854

Note that N will usually be a composite and thus not a prime. This, however , does not matter. An adversary intercepting a sent message M encoded by N will not be able to factor things since he has no idea what N is being used. One can think of the abbreviated form as a password very unlikely to be broken by any adversary using trial and error methods.

A few more examples for Ns are-

7LPSG=7{ln(2)*π*sqrt(γ)}=729924882993662859154461621172539621511169

2EFC2= 2{exp(1)*(1+sqrt(5))/2 *2^(1/3)}

=414759666368890867623205081103588019412632382151
and

5PCEG=5{π*(exp(1)*gamma)^(1/3)}

= 704687451851706231845141028134455848861816785

The length of the Ns should typically contain more digits than the message one wants to send in encoded form. It is easy to lengthen N by just using more digit expansions in its irrational number components.

SENDING AND RECEIVING ENCRYPTED MESSAGES:

Suppose a sender wants to send a message M to a friendly receiver. He sends out the encrypted form M(N1), where N1 is a time-sensitive number in a list of n known Ns. This same list of Ns will also be known to the receiver but no one else. The receiver divides the incoming signal by each of the n Ns on his list until one N is found which decodes the message. The receiver can reply with the message R using the encoded form R(N2). The original sender can quickly decipher this reply. The list of Ns can be changed at any chosen time interval to introduce extra security.

Let us demonstrate things for the specific case where-

N1=5SEPGL=955696341027271287691074303934017355053109854

Let the message be M=3572 so that the encoded outgoing message will be-

U= M(N1)= 3413747330149413039632517413652309992249708398488

This message will be undecipherable for anyone listening except the intended receiver who can decode things using his N list. The receiver performs the following de-coding operation-

$$M=U/N1=[341374733014941303963251741365230999224970839848 8]/[95569634102727128769107430393401735505310985 4]=3572$$

to recover the message. The receiver can now reply to the sender by the reverse procedure using his own reply R multiplied into his own choice N2. The original sender can easily decipher this message since he has the same list of Ns available. For security purposes it will be a good idea to replace the N master list at short time intervals.

U.H.Kurzweg
October 12, 2017
Columbus Day