CRYTOGRAPHY REQUIRES A MIRACLE TO DEFEAT

William B. Tripp, Ph.D., D.Th.

February 21, 2002

Our nation's security depends upon the ability to safeguard classified information, preventing our adversaries from acquiring knowledge about our intentions, methods, identities, capabilities, and many other subjects. One of the methods employed to secure this information is cryptography, which uses the principles of mathematics in probability in the formation of coding systems that encrypt sensitive communications. In fact, this is the domain of the world's largest security organization, the National Security Agency, which is responsible for the development, implementation, and oversight of all cryptographic systems used to protect United States government sensitive and classified communications.

The actual method in which this security is achieved is in principle quite simplistic—it is ultimately very simple mathematics—though the numbers are quite staggering, even utilizing older cryptographic systems. Using the old style computer "punched tape" as an example, it can be seen just how the protection can be relied on with absolute certainty (absent obviously, human failure). One particular protocol that the old punched tape computers used had sections of 32 columns, with 8 positions in each column, residing on one inch wide paper tape. Each "position" either had a hole punched through or did not; to the computer, this meant either a "one" or a "zero" in binary coding as the tape passed through the reading machine. Each position then has 2 possibilities.

Since each position has 2 possibilities, each column of 8 positions has 256 total possibilities for that column, shown in the math function below:

Position: 1 2 3 4 5 6 7 8

$2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 = 256$

Since there are 32 columns, the total possibilities for each section is calculated by multiplying the 256 possibilities of each column for the number of columns, or:

256 x 256 x 256 . . . etc., for 32 times, which equals approximately 1×10^{76}.

This is a number much too large for the human mind to understand; the total number of atoms in the entire universe is estimated to be around 10^{80}. There are multiplied billions of atoms in the ink in the period at the end of this sentence.

The communications protected in this hypothetical encoding could be analyzed by the comparison of the amount of time it would take to randomly arrive at the correct combination for the "key" used in encrypting the data. Here an arbitrary and incredibly high figure is developed for the number of combination "tries" for a given time period is used to determine the relative security of the information encrypted. For example, if there were only 60 combinations possible, and each "try" takes one minute, the relative value of one hour of "crypto-security" would be assigned. Considering the advent of high speed computers, capable of billions of calculations per second, the arbitrary figure of 100 trillion calculations per second would provide a wide margin of safety.

Assuming that the minimum crypto-security desired is ten years, the calculation would proceed as:
100 trillion/sec. x 60sec./min. x 60min./hr. x 24hrs/day x 365days/year x 10 years.

The total number of "tries" accomplished in the foregoing attempt is around 1.31×10^{22}, a very large number, but is still far short of the total of 1×10^{76}. To determine just how close the attempt came over the hypothetical ten-year attempt, the number of "tries" performed is subtracted from the total possibilities:

1×10^{76}
$- 1.31 \times 10^{22}$
1×10^{76}

Notice that the result of subtracting the combination "tries" from the total results in the same number as the total; with numbers this large, mathematics does not work in the same concepts most understand. Indeed, it is difficult to comprehend how a number such as 10 to the 22nd power (10^{17} is the state of Texas filled to two feet deep with half-dollars) removed from anything else has no effect on the answer. It does indeed have an effect, though the first number is actually so large that the difference between the two in this case is so small that a scientific computer, using exponential notation, cannot calculate it. In other words, given the total of "tries" (at 100 trillion per second for 10 years) it is the same as if no try at all had occurred; there is no chance at solution.

Another way of expressing the impossibility of randomly arriving at the correct combination can be seen by dividing the total (1×10^{76}) by the number of "tries" (1.31×10^{22}) which provides the number of cycles of the ten years would be required before all of the combinations had been tried. This equals approximately 10^{54}; which means that performing 100 trillion combinations per second for ten years would require 10 followed by 54 zero's repetitions of the ten-year attempt. Just 10^{12} repetitions would require 10 trillion years!

It would seem obvious and perhaps gross understatement to say that a miracle would be required to randomly or accidentally arrive at the correct combination; in our hypothetical cryptographic system, the security of our communications is quite safe. Yet this analogy is actually quite closer to every human's daily experience than most would believe, and much more important than one can imagine.

LIFE REQUIRES AN EVEN BIGGER MIRACLE

Evolutionists contend that various chemicals (conveniently collocated) bonded producing complex chains of enzymes, proteins, fats and fatty acids, among many other compounds, that eventually formed the first living cell. These chains are very much like the previous analogy of cryptographic systems in that quite literally, these compounds record information just as information is encoded in a cipher. In fact, this is how scientists believe DNA actually works, calling it the "Blueprint of Life," minor changes in the sequences having drastic results in the organism.

The evolutionary premise is that these compounds, gathered together in a precise, ideal environment, and given some "spark" or infusion of energy, formed the first living cell, the chains of enzymes, proteins, and DNA “accidentally” or randomly arranged in the one particular combination to achieve life. The mathematical analogy of the hypothetical crypto-system previously detailed can be used to illustrate the probability of this occurrence, thereby providing a relative certainty (or uncertainty) that the evolutionary stance is “safe.”

The minimum number of enzymes for the most simple, single celled organism to live is around 250; these enzymes exist in a sort of string, or perhaps better, a chain, each link being a particular enzyme which must appear at that particular position. Just as in the example of cryptography, margin of safety calculations are generally performed on an exponential order of magnitude; that is, where there could be failure, it must be on the side of security. With this in mind, the question of the relative certainty of the mathematical position of evolution can be analyzed.

In this case, the margin of safety will be excessive; instead of 250 enzymes, only 1/5th that number [50] will be used (this would be roughly equal to using only 7 columns instead of 32 in the previous model). Where 50 enzymes are present, there are 3×10^{64} possible combinations (using a factorial, which in addition, assumes that each unsuccessful “try” is not repeated; random chance actually means that they can recur). Even though this number is well above the “line of impossibility” (10^{55}) set by scientists to rule out the possibility of an occurrence, evolutionists usually respond with essentially, “given enough time, anything is possible.”

To this then the previous method can be applied to determine if that is indeed true, though the numbers will have to be “adjusted” to allow for the evolutionary scale of time. Scientists (evolutionary at least) believe that the earth is around 4.5 billion years old and required about 2 billion years to cool sufficiently to support life. Owing to the previous deference to the “margin of safety,” (and evolutionary theory needing all the help it can get) the original figure of 4.5 billion will be rounded up to 5 billion, and then multiplied by six, for a total of 30 billion years. The original arbitrary figure of 100 trillion tries per second will be retained, only instead of ten years, the process will cover the 30 billion year period. This yields a number around 2.82×10^{39}; obviously still short, though the subtraction will help understand how close the ridiculously high number of 100 trillion tries per second actually is. Therefore:

$$\begin{array}{r} 3 \times 10^{64} \\ - 2.82 \times 10^{39} \\ 2.999999999 \times 10^{64} \end{array}$$

In this case, the answer actually does change somewhat, though with numbers this large it is difficult to discern exactly how much, and in turn, how close the 100 trillion “tries” per second for 30 billion years actually came. The next step is to divide the total possibilities by the total “tries” in that period to determine how many times this 30 billion-year period would have to be repeated.

The number is actually quite staggering, and every bit as hard to understand as the original: 3×10^{64} divided by 2.82×10^{39} equals 1.06×10^{24}. What this means in actuality is that the 100 trillion tries per second for 30 billion years would have to be repeated a trillion, trillion times, or 1,000,000,000,000,000,000,000,000 times. In other words, the pace of 100 trillion tries per second would have to continue for 31,000,000,000,000,000,000,000,000,000,000,000 years, which is 60 trillion, trillion times the estimated age of the earth.

It should be remembered that the base used was only 1/5th of the total enzymes, calculated using a factorial, given 6 times the estimated age, and the ridiculous figure of 100 trillion tries per second. Further, not only are there 250 enzymes, there had to have been more than 2,000 proteins; the factorial alone of this number is around 3 x $10^{5,735}$ (notice that the exponent itself requires a comma). Indeed, Sir Fredrick Hoyle, an eminent British mathematician and scientist, calculated the odds against the random formation of the enzymes and proteins alone at $10^{40,000}$. Yet, this does not even begin to address the more than 3 million "positions" of DNA, with its 24 possibilities on each; this number is all but incalculable—most scientists believe the number would have an exponent that would have to be expressed in exponents!
It would seem quite "safe" to say that there is very little "security" in evolution, though in this case it is not just national security that may be in jeopardy, but rather one's eternal security. In other words, would you trust your life to such odds?

Probability and the Origin of Life by Robert E. Kofahl
http://www.parentcompany.com/creation_essays/essay44.htm

For roughly fifty years secular scientists who have faith in the power of dumb atoms to do anything have been carrying on scientific research aimed at finding out how the dumb atoms could have initiated life without any outside help. Since they believe that this really happened, they believe that it was inevitable that the properties of atoms, the laws of physics, and the earth's early environment should bring forth life. More sober minds, however, have realized the immense improbability of the spontaneous origin of life (called "abiogenesis"). Some have made careful investigations and mathematical calculations to estimate what the probability is for abiogenesis to occur. Their calculations show that life's probability is extremely small, essentially zero.

To understand these results let us explain what we mean by probability. What, for example, is the probability of tossing a coin and getting "heads"? There are two possible outcomes of tossing a coin, either the head side or the tail side will be up. The sum of the probabilities of these two outcomes is 100% or 1, unity. Then, since for a perfectly balanced coin the two probabilities must be equal, and their sum is 1, the probability of either heads or tails in one flip of the coin is ½ , and the sum of the two probabilities is ½ + ½ = 1. Simple. Now you understand probability!?

Now let's ask what the probability is for flipping the coin twice and getting two heads in a row. It is the product of the two probabilities of getting heads both the first time and the second time. That is, P2H = ½ x ½ = ¼. Now you understand how to calculate the probability that both of two independent events will happen. It is the product of the probabilities of the two events.

Next we will calculate a probability for the chance production of a single small protein molecule. A protein molecule consists of one or more chains made up of amino acid molecules linked together. There are 20 different amino acids molecules which the cells use to construct the protein molecules needed for the life of cells. We will think about a small protein molecule with only 100 amino acid molecules in its chain. Assume we have a reaction pot containing a mixture of the 20 different amino acid molecules, and they are reacting at random to form chains. What is the probability, when a chain with 100 amino acids is formed, that it will by chance have the sequence of amino acids needed to form a particular working protein molecule?

There are 100 positions along the chain. What is the probability that a particular one of the 20 different natural amino acid molecules will by chance be placed at position number 1 in the chain? It will be P1 = 1/20. When the complete chain has formed, what is the probability that the necessary particular amino acids will be placed at each of the 100 positions in the chain? It will be the product of the probabilities at the 100 positions. Thus the probability will be the fraction 1/20 multiplied by itself 100 times. So P100 = (1/20)x(1/20)x(1/20)x...x(1/20) = $(1/20)^{100} = (1/10)^{130} = 1/10^{130}$. This is an extremely small fraction. It is the fraction formed by the number 1 divided by the number formed by 1 followed by 130 zeros!

But we have oversimplified a little bit. In actual fact a protein molecule can have a substantial variability at many of the positions on its amino acid chain. In 1975 I examined the data for a particular protein molecule called cytochrome a which has about 100 amino acids in its chain. This is an important enzyme molecule in all living cells, and the sequence of amino acids has been determined for cytochrome a molecules in about a hundred different species. From the quantitative data I made a rough estimate that on the average up to five different amino acids could fill a particular position on the chain of the enzyme molecule. Thus the probability that an acceptable amino acid would be found by chance at a particular position would be 5/20 = ¼. So the probability for a working enzyme molecule to be formed by chance would be $(1/4)^{100} = 1/10^{60}$. This is still a very, very small probability. It is the fraction formed by 1 divided by the number 1 followed by 60 zeros.

In 1977 Prof. Hubert Yockey, a specialist in applying information theory to biological problems, studied the data for cytochrome 'a' in great detail.

1. His calculated value for the probability in a single trial construction of a chain of 100 amino acid molecules of obtaining by chance a working copy of the enzyme molecule is $1/10^{65}$, or the fraction 1 divided by 1 followed by 65 zeros. This is a probability 100,000 times smaller than my very rough estimate published two years earlier. Prof. Harold Morowitz estimated that the simplest theoretically conceivable living organism would have to possess a minimum of 124 different protein molecules. A rough estimate of the probability of all of these protein molecules to be formed by chance in a single chance happening would be P124P = $(1/10^{65})124 = 1/10^{8060}$, the fraction 1 divided by the number 1 followed by 8060 zeros. Truly these are extremely small probabilities calculated through a statistical approach. They tell us that the probabilities for the chance formation of a single working protein molecule or of a living cell are effectively zero. Prof. Morowitz made a careful study of the energy content of living cells and of the building block molecules of which the cells are constructed. From this thermodynamic information he was able to calculate the probability that an ocean full of chemical "soup" containing the necessary amino acids and other building block molecules would react in a year to produce by chance just one copy of a simple living cell.
2. He arrived at the astronomically small probability of Pcell = $1/10^{340,000,000}$, the fraction 1 divided by 1 followed by 340 million zeros! Yet he still believed in abiogenesis. Back in the 1970s Prof. Morowitz admitted in a public debate at a teachers' convention in Honolulu that in order to explain abiogenesis, it would be necessary to discover some new law of physics. At that time he still believed in abiogenesis, the spontaneous formation of the original living

cells on the primeval earth. However, some ten years later he finally stated that in his opinion some intelligent creative power was necessary to explain the origin of life.

There are yet more mysteries in life's probability(or improbability) which science has not plumbed. One mystery is how one virus has DNA which codes for more proteins than it has space to store the necessary coded information. A gene is a portion of the long DNA molecule which carries the code for the sequence of amino acids in a chain that folds up to produce a particular protein molecule. The DNA molecule is itself made up of four code letter molecules called nucleotides. These provide the four-letter alphabet of genetics. Their names are abbreviated by the letters A, C, G and T. A three-letter "word" called a codon codes for a particular one of the twenty amino acids used to build protein chains.

The mystery arose when scientists counted the number of three-letter codons in the DNA of the virus, fX174. They found that the proteins produced by the virus required many more code words than the DNA in the chromosome contains. How could this be? Careful research revealed the amazing answer. A portion of a chain of code letters in the gene, say -A-C-T-G-T-C-C-A-G-, could contain three three-letter genetic words as follows: -A-C-T*G-T-C*C-A-G-. But if the reading frame is shifted to the right one or two letters, two other genetic words are found in the middle of this portion, as follows: -A*C-T-G*T-C-C*A-G- and -A-C*T-G-T*C-C-A*G-. And this is just what the virus does. A string of 390 code letters in its DNA is read in two different reading frames to get two different proteins from the same portion of DNA. Could this have happened by chance? Try to compose an English sentence of 390 letters from which you can get another good sentence by shifting the framing of the words one letter to the right. It simply can't be done. The probability of getting sense is effectively zero.

Reasoning from these and other mathematical probability calculations, we can conclude that, without God the Creator, life's probability is zero.

Footnotes
1. H.P. Yockey, "A Calculation of the Probability of Spontaneous Biogenesis by Information Theory," J. Theoretical Biology, (1977), 67, pp.337-398.
2. H.J. Morowitz, Energy Flow in Biology (Academic Press, New York, 1968), p. 99.

Evolution, chance and creation

by Michael Stubbs
http://www.answersingenesis.org/creation/v4/i2/chance.asp

Many ordinary people believe that an uncontrolled process called evolution has produced the intricate designs which we see around us. It only takes a few moments of easy mathematics to check out the truth of such a belief.

A chance ratio of 50:50.
When we toss a coin, we expect it to land showing either a head or tail. We say from experience

that the probability of the coin landing 'heads' is one half, or we can say 'tails' has a 50% chance of showing up. We also know from experience that this does not mean when we throw a head first, the next throw will be a tail. It simply means that if we keep tossing coins long enough, then half the time the coin lands, it will show heads, and half the time tails.

However, even in the idea of '1/2 heads' are some assumptions or beliefs which few of us bother to check when throwing coins. We take it for granted that the coin weighs the same on both head and tail sides, so it gives an unbiased result. We rarely check to see if the coin has both a head and a tail, even though rare double headed coins do exist.

An interesting situation arises when two separate events occur at the same time, e.g. tossing a coin and throwing a die. (Most of you will call it a dice, but that is plural for more than one die.) If we ask what is the 'chance' of throwing a head and a 6 at the same time, a simple look at all the possible results of throwing coins and dice will show the answer. Since the coin has two sides and only one head, the possibility of a head is 1/2. Since the die has six sides and only one face with 6 on it, the possibility of six is 1/6.

The only trouble is that half of the times the die lands showing a 6, the coin will show a tail, the other half of the times we throw a 6, the coin would show a head. So the probability of throwing the head and the 6 together, must be one half of the sixes, or put mathematically, 1/2 x 1/6. This, of course, is 1/12. Again we must remember that this does not mean one in every 12 throws, but if you throw for long enough, 1/12 of all throws would have both a 6 and a head (see footnote). Puts one off gambling somewhat!

Can 'chance' count to 10?

Let us extend this idea further. (A problem for any Grade 10 math's class.) Suppose we have a bucket in which are placed ten (10) identical discs, each numbered from 1-10. The question is: Can chance methods enable us to count from 1 to 10? If only one disc is to be selected from the bucket, noted and replaced, and we require disc 1 first, disc 2 second, etc. in the correct sequence from 1-10, what is the probability of selecting all ten discs in order?

The maths are relatively easy. Since there is only one disc numbered 1, there can be only one chance in ten (1/10) of selecting it. After we replace the first disc, the chance of selecting the disc number 2 is the same—1/10. In fact, every separately numbered disc has one chance in ten of being selected. The probability of selecting the first one followed by the second one in correct order must be 1/10 x 1/10 or 1/100. To select all 10 in the right order the probability is 1/10 x 1/10 x 1/10 x 1/10 x 1/10 x 1/10 x 1/10 x 1/10 x 1/10 x 1/10 or $(1/10)^{10}$. This means that you would select the right order only once in 10 billion attempts. Put another way 'chance' requires 10 billion attempts, on the average, to count from 1 to 10.

The theory of evolution

Further tests exist to measure how efficient chance is at producing design. The following is fascinating. The question is: What is the expected probability for chance to spell the phrase—'the theory of evolution'? This phrase by chance would involve the random selection and sequencing of letters and spaces in the correct order. Each letter from the alphabet plus one space (totaling 27 possible selections) has one chance in 27 of being selected. There are 20 letters plus 3 spaces in the phrase—'the theory of evolution'. Therefore 'chance' will, on the average, spell the given phrase correctly only once in $(27)^{23}$ outcomes!!

This computes to only one success in a mind boggling 8.3 hundred quadrillion, quadrillion attempts ($8.3x10^{32}$) (gasp!). Suppose 'chance' uses a machine which removes, records and replaces all the letters randomly at the fantastic speed of one billion per microsecond (one quadrillion per second)! On average the phrase would happen once in 25 billion years by this random method. If, as evolutionists would have us believe, the earth has been in existence for approximately 5 billion years, then 'chance' could take five times this time to spell out its own success, even at this phenomenal rate of experimentation. And this phrase is infinitely simpler than the smallest life form, and children of average intelligence could perform this same spelling task within a minute or so.

Amended 7 October 2004.
Footnote

Statisticians have made this into a rule called the Multiplication Rule of Probability. This states that the chance of several independent results occurring at once is found by multiplying the mathematical probabilities of obtaining the individual results.

THE EVOLUTION OF LIFE, PROBABILITY CONSIDERATIONS AND COMMON SENSE
By Dr. John Ankerberg and Dr. John Weldon
http://www.ankerberg.com/Articles/_PDFArchives/science/SC1W0202.pdf

---

THE MATHS OF PROBABILITY – The Mathematics of Probability Refutes "Coincidence"
http://www.creationofuniverse.com/html/equilibrium03.html

THE PROBABILITY OF THE OCCURRENCE OF A UNIVERSE IN WHICH LIFE CAN FORM is 10^{10123} as calculated by Roger Penrose, a famous British mathematician. According to Penrose, the odds against such an occurrence were on the order of 10^{10123} to 1. By reference this is more than the total number of atoms 10^{78} believed to exist in the whole universe. In practical terms, in mathematics, a probability of 1 in 10^{50} means "zero probability". Penrose's number is more than trillion trillion trillion times less likely than that. In short, Penrose's number tells us that the 'accidental" or "coincidental" creation of our universe is simply stated "an impossibility". This now tells how precise the Creator's aim must have been, namely to an accuracy of one part in 10^{10123}. This is an extraordinary figure.

The American astronomer George Greenstein confesses this in his book The Symbiotic Universe:

> How could this possibly have come to pass (that the laws of physics conform themselves to life)?…As we survey all the evidence, the thought insistently arises that some supernatural agency - or, rather Agency- must be involved. Is it possible that suddenly, without intending to, we have stumbled upon scientific proof of the existence of a Supreme Being? Was it God who stepped in and so providentially crafted the cosmos for our benefit? Page 27

http://www.creationofuniverse.com/html/equilibrium03.html

Rebuttal on assumptions of probabilities at:
http://www.talkorigins.org/faqs/thermo/probability.html

Another rebuttal with some strange conclusions:
http://www.freethoughtdebater.com/FComplexityProbability.htm
