All Summer Long

Perhaps the highlight of our social life has become the business of trawling through charity shops for items of interest.

I was never one for reading history, but came across a gift set of the Pan "*Grand Strategy*" series about WWII. The books had never been opened which was not surprising. How they came to exist in this part Ireland is one of Mother Nature's great mysteries. The books had swollen with damp to the point of bursting their presentation box. The original price was £80 which I would never have handed over for a bunch of history books even in the days when I could afford it. However, €4 was just on my limit, so I took the gamble. It turned out to be one of the best purchases we've made this year.

The book that drew my attention was Station X by Michael Smith. The book tells the story of Bletchley Park. I would have slotted into that environment perfectly. Working on the Colossus project would have been my dream job, and it produced a real payoff for the war effort. Funny thing is, I am not really interested in cryptography. I studiously avoid crossword puzzles. The clues are invariably meaningless to me. When I was 16 years old, working in my first job, one of the girls would do the crossword at tea breaks. We would all be sitting quietly until Annette broke the silence by announcing some clue which might be "*This man is extremely close*" together with something to the effect of "*blank blank R blank blank blank R*". I would identify "*Vernier*" in an instant. I wasn't working from the clue, but simply slotting in letters from words I knew and then checking any possibles against the clue. I was totally unaware of the process I was employing until years later. It was like playing chess. Only the end game ever had any meaning to me. The rest of it was just an exercise in clearing pieces off the board – usually mine.

More than ten years ago I read "*The Code Book*" by Simon Singh. I bought it when I was stuck in an airport departure lounge. The most interesting item in the book related to the Diffie-Hellman key exchange algorithm which had become the standard for Internet communications. It transpired that GCHQ had devised the same algorithm some years prior to Diffie and Hellman but British Intelligence never made use of it. The reason seems obvious once it is explained, but apparently neither Diffie nor Hellman could see the fatal weakness that GCHQ staff had evidently identified.

It took me a while to identify the flaw too. However, I am not a cryptography devotee, and it seems incomprehensible that specialists such as Diffie and Hellman were unable to spot the weakness.

This begged the question: Why base Internet communication on an "*Insecurity*" key exchange protocol? The answer may lie in a quote from the film "*The Fifth Estate*":

"*Man is least himself when he speaks in his own voice – but give him a mask and he will tell you the truth*".

The quote given above can be interpreted in a number of ways. Confidence tricksters continually rely on a "*Mask*" in order to deceive. The "*Mask of respectability*" is the first choice of criminals. Many such people achieve wide recognition and high social status. One need only think of such people as (Sir) Jimmy Saville, Dr Harold Shipman, or Jack the Ripper, to realise the effectiveness of the mask of respectability.

Intelligence services exist for the purpose of spying. If they do not exploit every possible technique to that end, they are failing to meet their obligations. The appearance of computer networks represented a mechanism whereby subversive elements in society might communicate freely. By providing something which purported to be a "*Mask*", but was in fact transparent, the Intelligence Services retained confidence in their ability to monitor communications, while those attempting to conceal secrets would believe in their own ability to do so. Such was the real genius of the key exchange algorithm.

Key exchange was only one part of the problem facing secure communication pundits. A second was the cryptographic mechanism employed by those communicating with one another. Bletchley Park expended an inordinate amount of effort to discover the internal mechanism of successive Enigma variants. They were given a head start by the Polish Cryptanalysts prior to the outbreak of WWII. The threat of having to analyse an ever changing variety of cryptographic techniques was partly addressed by arguing that the robustness of the key was security enough, allowing everyone to use the same encryption algorithm. This Herring was Scarlet with embarrassment in its nakedness, so it needed to be clothed in the "*Factorisation Problem*" which was perhaps the biggest selling point of Internet cryptography.

The difficulty of factorising a number increases with the square of the number itself. That means that if the cryptographer uses a big enough number for the key, the code cannot be cracked in an acceptable time. Factorisation is classified as "*Intractable*" in contrast to a "*Tractable*" problem, the difficulty of which only increases in proportion to the size of the number. Of course, "*Tractable*" is much tougher than "*Direct*". The latter means that the effort involved in finding the solution is not affected by the size of the number.

The factorisation problem is quite awe inspiring, and it was 2007 before I devised an algorithm which reduced factorisation from intractable to tractable. I would have liked to have reduced factorisation to the direct level, but was nevertheless quite pleased with my achievement.

However, the Factorisation problem might as well not have existed. It is virtually inconceivable that specialists who devote their entire lives to codebreaking could not achieve what I managed by way of mathematical

amusement. Factorisation closed the back door to Internet security while the flaw in the Key Exchange algorithm together with unified encryption methods ensured that the front door would always be wide open.

The difficulty of persuading people to adopt a transparent mask may have been addressed by "*Pretty Good Privacy*" (PGP). This software was made available free of charge by an individual, so it appeared to be devoid of any "*Shadow*" of Government duplicity. Widespread adoption was effectively guaranteed by a Federal Court Action against the software author. However, the Court Action was apparently dropped after a while. It is possible that the PGP saga was nothing more than a clever ruse by the American Intelligence Services.

Gary McKinnon, a young man from Glasgow, crashed the NASA system while he was fooling about looking for evidence of UFOs. The entire might of American Legal Bureaucracy was brought to bear on this unfortunate person who had the decency to own up to what he had done. Nobody stopped to ask why the American taxpayer had handed over huge sums of money to a private corporation for a secure communication system which could be brought down by a person with limited formal training in computing.

A couple of years ago there was an advertisement by the British Government for computing specialists to join the Volunteer Reserve. The Advertisement stated that there were approximately 20,000 cyber attacks on UK Government systems every month of which 5% posed a "*Serious threat*" to military security. The advertisement was a beautiful illustration of the appalling fragility of critical defence systems. Apparently all communications security systems are founded on the fundamental principle that "*Everyone will do as they are told*". One might argue that the principle is not a terribly sound basis on which to proceed.

Angela Merkel complained loudly about the Intelligence services eavesdropping her telephone conversations. As a Physicist, Ms Merkel ought to have had sufficient understanding of technology to expect eavesdropping. Furthermore, as the German Chancellor, she would have been furious had her own country's Intelligence Services been failing to eavesdrop on other political leaders. Ms Merkel's tantrum was somewhat amusing in some respects. Above all others, leading public figures are the very ones whose lives ought to be subjected to the closest scrutiny. These individuals have chosen Public life for their own ends. There is ample evidence to show that corruption and high office coexist. There are those who would argue that it is not power which corrupts, but that people of a corrupt nature are those most likely to seek power. The Electorate deserve to have confidence that Public Figures will not dare to conduct themselves in any manner which could become a threat to National Security. Had anyone been paying the slightest attention to Tony Blair's agenda, Britain would not have been "*Misled*" into the second Gulf War.

Acceptance that communication is insecure is now fairly widespread. Some people make a very good living from the simple expedient of hacking into corporate systems, and shutting out the legitimate users. The corporation is obliged to pay a ransom to have the "*Hostage computer*" released. Fear of shareholder reprisal tends to prevent CEOs from pursuing the perpetrators. Those in charge of major companies are unlikely to relish the prospect of losing their salaries and bonuses, even if the shareholders pay dearly for failures at Board level.

When I was an undergraduate I had a Summer job at a factory near London. The locality was as close to being a ghetto as anything I ever want to experience, and the factory itself was a dive. I was shoehorned into a cubicle about 2'6" x 6' in an open plan office / lab arrangement. Brain compression started to set in immediately. I was handed a computer program written in Basic and told to figure out how it worked. It was patently obvious that the programmer had known nothing about structure or documentation. The situation was exacerbated by the primitive nature of the Basic language.

After a while I began to construct a flow chart. Perhaps it should have been called a "*flaw chart"* since it became clear that whoever the programmer had been, he or she hadn't known much about programming at all. The company didn't have its own computer and used a teleprinter connected to an agency service by a land line. It was an exceptionally clever arrangement. The program was supposed to be working out transfer functions for an optical system used on military aircraft. If the program had any merit at all, it was to broadcast technical secrets to anyone who cared to listen. Mind you, I couldn't see any technical merit in the program, even with the source code in front of me. - Heaven help the poor eavesdropper. It was obvious to me that it would have been much more efficient to present me with the original problem and to let me solve it in my own way ab initio.

While I was figuring out the purpose of the program I had been given to work on, I didn't need to use the teleprinter. That created a bit of a problem. Few people understand that good programming is carried out away from the keyboard. Some of my best computer algorithms were developed while I was lying awake in my bed in the wee small hours. However, the boss evidently thought I was just sitting at my desk doing nothing. Consequently, I escaped by going to the teleprinter cubicle. To get me up to speed on using of the service, I wrote a little program of my own.

Coca Cola were running a competition that year with a Lotus Europa sports car as first prize. The objective was to see how many words could be made from the letters of the phrase "*All Summer Long*". In those days, competitions had an intellectual component. It was possible to believe that they were something more than lotteries devised to supply marketing statistics and sales leads. There was more to making an entry than scratching silver foil from the surface of a card or filling in personal details and putting an "X" in the only box provided.

Scrabble is anathema to me. Many words were fairly obvious – gum, smog, learn, manger, rummage, to mention a few. Considering the restricted choice of letters, and the value of the prize, a manual scan of the Oxford English Dictionary represented a systematic and very workable approach to the main part of the competition. However, the entrant was also required to suggest a possible English word which utilised all the letters. I saw the puzzle as a programming exercise. I didn't get any pay for my nocturnal efforts, and I wouldn't have been in front of the teleprinter at all had the boss been in possession of a second neuron, so it seemed fair do. The given phrase contains 13 letters, which limits the number of possible permutations to a mere 6,227,020,800. Not all of these permutations are distinct either.

Naturally there are certain rules to the English language (so I am told). For example, every word should have at least one vowel (unless it doesn't). There are very few singular words with three consonants appearing together. Exceptions are restricted to certain patterns such as "*Thr*" as in "*Three*". The possibility of four or more consonants in a row could be ignored for singular words. The consonants available in the competition were limited to l,s,m,r,n, and g. A permutation of any three from six provides 120 triples in which all the characters are unique. Consonant triples with two identical letters, even if they were not adjacent, did not look terribly likely as a component of a word in the English language. Similarly vowels seldom appear in triples, though "*Queue*" flaunts this rule. Four of the vowels were available, providing only 12 permutations of doubles. The given phrase itself contained a lot of redundancy. There were 3 instances of the letter "L" for example. It was fairly clear that patterns such as "*glllmmnrs*" in which all the consonants appear together were not good candidates for possible English words. There are 362880 permutations in this nine letter group. The vowels "*aeou*" can be arranged in 24 ways. Thus an arrangement like "*aeouglllmmnrs*" in which all four vowels are immediately followed by the nine consonants would generate 8,709,120 irrelevant patterns.

All 13 letter pattern variants were repeated 12 times on account of the triple "L" and double "M". The repetitions did not need to be considered. The majority of patterns could be eliminated by suitable programming expedients.

I decided to start with words of 4 letters, partly for the purpose of testing my program, but mostly because it matched the limit of my linguistic ability. I set up some loops, coded in exclusion rules, and organised formatting for the output. Off it went – clatter clatter clatter – ten characters per second. It was flying!

Despite the exclusion rules I had incorporated, there were still innumerable patterns which were not words of the English language. Computer based dictionaries were not available, which called for a manual search of the output. I soon came to my first success - "*ARSE*"! This was an omen. I logged off, collected my belongings, and said goodbye to that factory forever.

I didn't bother to enter the competition in the end, though I eventually came up with a potential word which used all the letters: "*Gresullmonalm*". Noun: An obligatory disbursement, made with considerable anger and resentment to a recipient who neither needs nor has any legitimate right to the sum involved. Examples of a gresullmonalm could be Bank charges, Lawyers' fees, or contributions to aggressive charity collectors. The potential for related words is considerable. The adjective "*Gresullmonary*" and the infinitive "*To gresullmonate*" are only two examples. People who indulged in the practice would be "*Gresullmonists*" and the systematic study of the subject would of course be "*Gresullmonology*". Individuals who became depressed as a result of being the victim of incessant gresullmonary behaviour on the part of others might be said to be suffering from "*Gresullmonotony*".

Thinking about the competition provided me with quite a bit of amusement. Only when I read The Code Book did I discover that techniques I had devised about a quarter of a century earlier had some commonality with the methods used to penetrate the German cyphers during WWII. One thing that pleased me in reading the story of Bletchley Park in Michael Smith's book was to discover the level of refinement which the Russians had achieved in their teleprinter communications technology. Many people regard German technology as the best that money can buy, but the Russians had incorporated frequency multiplexing into their teleprinter system! As in so many technologies the Russians were years ahead. Germany found out the hard way just how good Russians technology can be. Britain only retained its freedom through WWII as a consequence of the Russian sacrifice. Churchill understood that from the outset.

I was once told that the USA developed the Phantom aircraft during the Vietnam war because Russian MIGs outperformed every fighter the West could produce. Anyone who has watched the "*Cobra*" manoeuvre at an air display can only marvel at the robustness of the aircraft and the physical endurance of the pilot. After the USSR dismantled the Berlin wall, there was a veritable flood of interesting Soviet technology to the West and Russian programmers were immediately respected for the efficiency of their code. The Soyuz rocket quickly earned a reputation as the most reliable of satellite launch vehicles. While some people may scoff at the "*Kremlin Memorial Flight*" of ageing Bear aircraft, patrolling international airspace around the UK, it is worth remembering that the West would have considerable difficulty keeping *any* of its Cold War era aircraft aloft! The Bear is a well proven platform. Who can guess what delightful technology awaits the unwary should they anger this majestic princess of the sky?

Jim Cahill