From the memoirs of a Norwegian cryptologist

Ernst S. Selmer
Idrettsvegen 20, N-1400 Ski, Norway

Norwegian cryptology was first organized, in the 30's, by then Capt. R. A. Roscher Lund. He set up a "Cryptology club", recruited partly from amateurs, partly from mathematicians. Many members came from a bridge club with the appropriate name "Forcing". Around the outbreak of the war a "Defense information office" was established with some (very) few cryptologists.

Personally, I was too young then, and first met cipher work during the war. My friend *Nils Stordahl* was strongly involved in the Norwegian underground movement, which needed secure communication with Stockholm. Stordahl recruited me and some other students of mathematics for a cipher service. Under the circumstances, only a hand cipher on letters was possible. The actual types are a transposition (letter permutation) or a substitution cipher. Our underground system in Norway was based on transposition. The letters of a key word (or key phrase) are numbered from their position in the alphabet, for instance

S	E	L	M	E	R
6	1	3	4	2	5
M	A	R	Y	X	H
A	D	X	A	X	L
I	T	T	L	E	X
L	A	M	B		

(X between words could be dropped.) The cipher text is then read off column by column in the numbered order.

The result is a single transposition, which is reasonably simple to break. We therefore used a *double transposition*, with a new key word on the result of the first step. I have read later that one should use key words of length 20–30, and messages of several hundred letters. Further, the text below the key numbering should not fill complete rectangles.

It is very easy to make mistakes in the transposition. My first encounter with cipher was extremely tedious and boring! But of course, we were glad to be of some use during the occupation.

T. Helleseth (Ed.): Advances in Cryptology - EUROCRYPT '93, LNCS 765, pp. 142-150, 1994.

Late in 1943, the Germans closed the University of Oslo and arrested the students they got hold of. I managed to escape to Sweden. There was my friend Stordahl already, and he saw to it that I got more cipher training before I was sent to London (where I arrived in the Spring of 1944 together with the first flying bomb, V1).

The already mentioned Roscher Lund had organized a Norwegian cipher network abroad, especially between Stockholm, London and U.S.A. The communication was mainly on the *Hagelin* cipher machine. This was a great success all over the world. At the end of the war, the U.S. army had 140,000 machines, and the producers, the Swedish Hagelin family, had become very wealthy.

In addition to some purely mechanical versions, there was also an electrical model with keyboard, which we were using in London. I was on a course in the Hagelin factory in Stockholm, and had just taken an electrical machine into parts and pieces, when Hagelin senior passed by. Addressed to me, he said that "it is easy to take it apart, more complicated to reassemble it, and much more difficult to make it work afterwards". But the next day, I could show him a working machine. The unforeseen result was that later, the complete technical responsibility for all Norwegian military and diplomatic cipher machines in London was put on top of my other duties.

The actual ciphering work on the Hagelin machines was only slightly less boring than the earlier double transposition. In the beginning, it was very exciting with all the military and diplomatic secrets you could read about. Very soon, however, one becomes completely blasé.

Roscher Lund's cryptologists had suspected that the Hagelin cipher might be broken, at least from corresponding plaintext and cipher, that is, from pure key. We therefore shuffled different parts of each message, and used a strange mixture of — often abbreviated — Norwegian and English. After the war, we learned from German archives that they had not been able to break our Hagelin cipher.

When the war ended, I was sent to Tromsø in Northern Norway as a cipher officer. But there was no need for cipher, so I spent a fabulous Summer under the midnight sun. I managed to get hold of some of the famous German *Enigma* cipher machines, and took them with me to the military headquarters in Oslo. But if I had been smart, I should have kept them for myself. Since the story of the Enigma breaking became publicly known in the 70's, the prices of old Enigmas have exploded. I have heard mentioned auction prices of $15,000 for a unit.

In 1946, Stordahl became head of the military cipher office, a position he held until 1983. He died much too early, in 1984. I always considered him my best friend. One of Stordahl's early initiatives was to engage me as a consultant. My first big task, and my most fantastic cryptological experience, was to establish a (hopefully) safe communication system for the Norwegian equivalent of MI5 and Scotland Yard Special Branch ("Overvåkningspolitiet" = "watch-over police"). We based it on the German Siemens teleprinter ("Fernschreiber"="remote writer"), with an additional unit for encryption/decryption (*"Geheimschreiber"* ="secret writer"). There were many of them in Norway, and the Norwegian (public) Telephone and Telegraph Company had collected them to dismantle the cipher unit and use them as ordinary teleprinters. We had to prevent this, and could not let it pass official channels. I cooperated with another of Stordahl's men, a young electrical engineer named Asbjørn Mathisen. Some time in 1946, we were supplied with two large military trucks and 20 German prisoners of war. We commanded them in our school-German, and drove to the Telecompany store just outside Oslo. The few attendants protested vigorously, but did not stand a chance against us and the Germans. Including a wooden case, each G-Schreiber weighed 180 kg, so the POW's were really needed. We got everything onto the trucks and drove it to a safe hiding place.

Mathisen used wires and torch bulbs to reconstruct the coupling diagram of the G-Schreibers, including 20 relays. I knew absolutely nothing about relays then, but had to find out how everything worked, from a maze of unsystematized wires.

The same reconstruction has been performed much later by other people. The Norwegian Technical Museum in Oslo had managed to get hold of 3 G-Schreibers. Two of them were given — for exchange purposes — to museums in London and Munich, and these were analyzed by Donald W. Davies in *Cryptologia* 6,7 (1982,1983). Some more historical information was supplied by Wolfgang Mache in *Cryptologia* 10 (1986).

The cipher unit contained 10 large notched wheels, stepped by a pawn mechanism. The number of steps in a revolution varied from 47 to 73, all pairwise coprime. The cam pattern was the same for all machines. The cams activated two contacts for each wheel. Over 20 relays, one contact set controlled an irregular stepping of the cam wheels, while the other set performed the ciphering of each 5 bit teleprinter symbol, in two rounds: one bitwise addition key, and one permutation (only 32 out of the 5!=120 were used). Details can be found in the Cryptologia papers.

I did not want to use the German outfit exactly as it was, so I made some modifications which Mathisen implemented. I could not change the notched wheels (with contact sets), but I fiddled with the above-mentioned relay control of the cam wheel stepping. I thought I made it more complicated, but had nobody to check whether the outfit had become cryptologically stronger.

The G-Schreibers came in successive versions 52 a/b, c, d, e. The first version was broken by the Swedish mathematician Arne Beurling (cf. *Kahn: The Codebreakers*) from the traffic passing Sweden between Norway and Germany. Later versions were "occasionally, but not routinely" broken by the British cipher office at Bletchley. — All this has become known later; in my case, I just had to hope for the best.

In my later designs of cipher machines (for NATO), I always said like the waiter: "Not my table", about all questions regarding protocols, key distribution, initiating and closing routines, etc. But for the police cipher, I had to work this out all by myself. In 1948, we summoned 20 police officers from different stations to Oslo, where I drilled them in the use of the G-Schreiber for a 3 weeks course. And the system was used from 1949 until around 1960.

I spent 1951 and the first half of 1952 in U.S.A. with a Rockefeller grant, to study computers, primarily von Neumann's famous Princeton machine. It became operative in January 1952, and I got the opportunity to run some of my number theoretical problems (indeterminate equations) on it. My programs were in fact the first ones to go through on the machine without any programming errors.

The machine had no printer, so we read off the numerical results from a display of lamps, arranged hexadecimally. In this connection, von Neumann made one of his very few errors: He wrote that because of the computers, humanity should be prepared to switch from the decimal system to numbers in base 8 or 16.

While in U.S.A., I was asked by a medium sized electronic company — on von Neumann's recommendation — to perform the logical design of a commercial computer. I undertook the job, which was finished after my return to Norway. I actually did the design down to every single tube (no transistors existed then). The company wanted a completely decimal machine, with a magnetic drum as its main memory. After a while, the company got economic problems and was swallowed by Burroughs, who entered the computer race with "my" machine *Burroughs 205*. In the late 50's, this was the most serious competitor to the famous *IBM 650*. My

machine was perhaps the only, and certainly the last, larger computer where the complete logical design was a "one man job".

Returning home in 1952, I told Stordahl that we needed a military computer in Norway. The next day, he came back to me and said that he had 1 million Norwegian kroner at his disposal! The whole affair was extremely hush-hush, with money paid secretly from U.S. to Norwegian intelligence, for Russian communication intercepted in Northern Norway. Anyway, the result for us was a Ferranti Mercury computer, which after some delay was installed at our Defense Research Institute in 1957.

Already in London during the war, I had been working on how to break the Hagelin machine cipher, at least with "normal" plaintext (and not distorted as we used in London). I continued with this after the war, and it was quite clear that only manual calculations would be too time-consuming. In 1952, I still did not have an electronic computer at hand, but now I did at least know very much about computer design. I used this to draw a special purpose relay computer, earmarked for breaking the Hagelin cipher. It was built by Finn Didriksen in Stordahl's office, and was used for several years breaking the diplomatic cipher of some foreign countries.

It is unnecessary for me to go into details with the Hagelin machine, which is described over 60 pages in *Beker & Piper: Cipher Systems*, including the breaking both with and without known plaintext. They refer to two papers from the late 70's. I have not studied these; it sufficed for me that I did the same job 25 years earlier.

Let me mention an interesting incidence from the 50's. The Norwegian Standard Telephone and Cable Company (STK), then a subsidiary of ITT, planned to build a one time cipher system based on 5 hole teleprinter tape. But how, in those early days, to generate a completely random binary sequence? A young Norwegian officer, Bjørn Rørholt, got the idea to use radiation from a radioactive source (cobalt). The project was very successful, and about 2000 one time cipher units were delivered before paper tape became obsolete. A "radioactive factory" produced the tons and tons of one time paper tape necessary to support the units. The most famous connection was the *"Hot Line"* between Kremlin and the White House (but the type of equipment for this line was not disclosed until many years later).

To generate a random binary sequence, the Germans had tried to read off a very quickly oscillating circuit with pulses from a slow one. We were two young Norwegians who went down to Germany to look at this concept. The result was negative, except for one experience: We met Hitler's famous (notorious?) chief of intelligence, *Gehlen*, who after the war had been recruited by U.S. intelligence.

In 1957, I left the University of Oslo to take over the position as a (full) professor of pure mathematics at the University of Bergen. Here my two NATO ciphers were "born". In the late 50's, I was asked to study the theory of *linear shift registers*, to use them for a cipher system which Standard was to build for the Norwegian forces. The subject was new to me, but I quickly caught up with the existing theory. The word "cipher" was hardly mentioned in the literature (although shift registers must have been used in cipher machines before 1960). I had to discover myself that with pure key known — which is always assumed today — breaking a system of purely linear registers amounts to solving a set of linear equations. So nonlinearity would be necessary somewhere in the system. But I also discovered what today is well known, that nonlinear feedbacks may lead to very short periods. What I ended up with was a design which today would be characterized as completely conventional: A series of binary linear registers with maximal sequences guaranteed a very large period. On the output of these came some nonlinear components, a system which today is usually called "feed forward". — You may perhaps say that my work then was a part of forming today's conventions.

Since Norway is a NATO country, my cipher machine needed acceptance by National Security Agency (NSA) in Washington. Fortunately, it passed the test without comments or corrections. It was then produced by Standard under the name *"Cryptel"*, and was used for many years. The engineers in charge of the project at Standard were Kaare Meisingseth and Per Abrahamsen.

The theory of linear shift registers was so interesting that I went on with it, both at home and during a sabbatical year 1964/65 in Cambridge, England, where I lectured on the subject. The lectures appeared in duplicated form at the University of Bergen in 1966, under the name *"Linear Recurrence Relations over Finite Fields"*. Since then, a series of (unaltered) editions have been produced, to meet the demand. My lectures must hold a world record for the number of copies of a duplicated monograph. Many of my cryptology friends call it their "bible" of linear recurrence — or at least the Old Testament. If we study Ch. 5 in Beker & Piper, we will see that they have landed exactly on my notation.

As already mentioned, I had to find out myself about the nonlinear parts of the Cryptel cipher machine, and use them in a feed forward system. Life would be much easier for a cryptologist if someone could establish a comprehensive theory about periods, cycles etc. for nonlinear registers. In

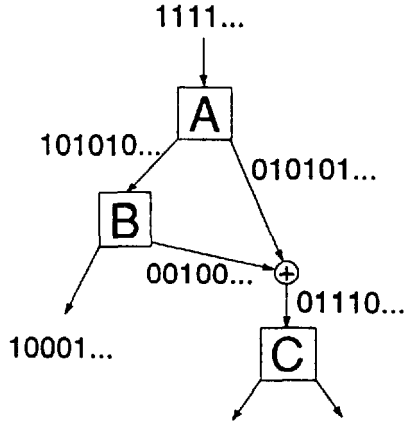
an attempt, I asked my student Johannes Mykkeltveit to look more into this. From my cryptological point of view, the result was negative. However, the project led to Mykkeltveit's well known proof of Golomb's famous conjecture about the maximum number of cycles generated by a linear or nonlinear register. (The maximum is attained for the pure cycling register.)

In my book, I was only able to solve completely one particular aspect of nonlinearity: *Multiplication of the output* of two linear sequences in a particular case. If the sequences have minimal polynomials $f(x)$ and $g(x)$, it is easily seen that any product sequence is generated by what I called $f \S g$, the polynomial whose roots are all the products of one root from $f(x)$ with one from $g(x)$. My main result, over an arbitrary finite field, was that $f \S g$ is irreducible if and only if $f(x)$ and $g(x)$ are irreducible polynomials of coprime degrees. This was the start of a long line of papers on such multiplication problems.

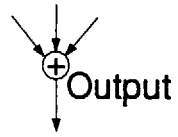
I have also joined the design of another NATO-approved cipher. This time, it was no one man job, but a teamwork where my part was more modest.

An officer at the naval base in Bergen, Cato Seeberg, had sent a suggestion for a machine cipher to Stordahl's office. His cryptologists turned the thumb down, but as a comfort, they asked him to contact me, since I was working in Bergen. I realized that the concept was new and original, and might be developed into a strong cipher.

Seeberg used a directed graph, with flip-flops and binary adders as components. The input flip-flop is triggered continuously. Each pulse makes the unit flip from one side to the other, and the incoming pulse passes out of the flip-flop on the side determined by its state. In the drawing, it is assumed that both flip-flops (nodes) A and B start in the "left" state.



We do not want the graph spreading out continuously. On the contrary, some pulse paths are collected in adders. In particular, a final adder gives just one output of the graph.



The inputs may come from different "levels". The final output can then be used to construct a key sequence. If there are n flip-flops, the number of different states of the graph is 2^n, so the output must be periodic.

There are two paths to the node C above, of lengths 1 and 2. If the longest path to the output has length l, then the period of the output sequence is at most 2^l. We want this to be independent of the initial state of the graph when the pulsing starts. A sufficient condition for this is that among the paths to any node, there is always just one of greatest length. In this case we can call 2^l the period of the graph.

After my positive reaction, Stordahl's cryptologists Kjell Kjeldsen and Ben Johnsen started working on Seeberg's concept. It was clear that the period length 2^l was too short, and it was increased as follows: Each flip-flop was replaced by a circulating binary sequence, which steps once for each incoming pulse. The 1's and 0's in this sequence then replace the sequence 1010... of flip-flop states.

Johnsen and particularly Kjeldsen made an extremely sophisticated analysis of the output from a modified Seeberg graph. Three papers were published in *Information and Control*; one by Kjeldsen (1976), one by Johnsen (1974), and a first common paper in 1973.

The periodic output sequence should obviously have a distribution of 1's and 0's as even as possible. The most important condition for this is that the output from the binary "skeleton" (Seeberg's original design, with only flip-flops) should have a completely even distribution. We had not obtained this when Kjeldsen, Johnsen and I went to Washington in 1971 to get an approval for NATO use from the NSA. One evening, the other two went to a movie (Marx Brothers), but I stayed in my hotel room to look more at the distribution. And suddenly it struck me that inclusion of just one more flip-flop in our suggested graph gave an even distribution. It was one of those aha-experiences which you never forget.

There are of course many other details which I cannot go into. The cipher machine got its NATO approval, and the electronic company *Lehmkuhl* took over the production of the so-called *"Omnicoder"*. Up to now, they have sold about 2000 units.

Until fairly recently, cryptology and cryptologists were very hush-hush. I was not allowed to declare my income from the consultant job in Stordahl's office! (The arrangement was cleared with the Auditor-General.) I did not earn more from the tax exemption, since my salary was adjusted for this.

As I remarked earlier, the word *cipher* did not turn up in the early literature on shift registers, not even in my textbook from 1966. Let me use the Omnicoder to illustrate how things suddenly became more relaxed.

I mentioned the papers by Kjeldsen and Johnsen. As mathematics, they were excellent, but many readers might ask what it is all about.

Kjeldsen added three more papers on cascade coupled sequences, and used this to get his Dr.philos. degree at the University of Bergen. Our degree is different from the American Ph.D. We have no oral examinations, but the requirements for the publications are higher. During the disputation, two opponents are dissecting the candidate's contributions, asking and criticizing.

Kjeldsen's disputation was in 1978, and I was one of the opponents. Since his 1976 paper, the secrecy of the *word* "cipher" had suddenly disappeared. Kjeldsen could now tell freely that he was working at the Defense cipher office, and in my introduction as opponent, I could explain his graphs in the same way that I have done above.

As you all know, the relaxing trend has accelerated. Just think of these international crypto seminars.