The Alice and Bob After Dinner Speech

given at the Zurich Seminar, April 1984, by John Gordon, by invitation of Professor James Massey

Good evening Ladies and Gentlemen.

There comes a time when people at a technical conference like this need something more relaxing. A change of pace. A shift of style. To put aside all that work stuff and think of something refreshingly different.

So let's talk about coding theory. There are perhaps some of you here tonight who are not experts in coding theory, but rather have been dragged here kicking and screaming. So I thought it would be a good idea if I gave you a sort of instant, five minute graduate course in coding theory.

Coding theorists are concerned with two things. Firstly and most importantly they are concerned with the private lives of two people called Alice and Bob. In theory papers, whenever a coding theorist wants to describe a transaction between two parties he doesn't call then A and B. No. For some longstanding traditional reason he calls them Alice and Bob.

Now there are hundreds of papers written about Alice and Bob. Over the years Alice and Bob have tried to defraud insurance companies, they've played poker for high stakes by mail, and they've exchanged secret messages over tapped telephones.

If we put together all the little details from here and there, snippets from lots of papers, we get a fascinating picture of their lives. This may be the first time a definitive biography of Alice and Bob has been given.

In papers written by American authors Bob is frequently selling stock to speculators. From the number of stock market deals Bob is involved in we infer that he is probably a stockbroker. However from his concern about eavesdropping he is probably active in some subversive enterprise as well. And from the number of times Alice tries to buy stock from him we infer she is probably a speculator. Alice is also concerned that her financial dealings with Bob are not brought to the attention of her husband. So Bob is a subversive stockbroker and Alice is a two-timing speculator.

But Alice has a number of serious problems. She and Bob only get to talk by telephone or by electronic mail. In the country where they live the telephone service is very expensive. And Alice and Bob are cheapskates. So the first thing Alice must do is MINIMIZE THE COST OF THE PHONE CALL.

The telephone is also very noisy. Often the interference is so bad that Alice and Bob can hardly hear each other. On top of that Alice and Bob have very powerful enemies. One of their enemies is the Tax Authority. Another is the Secret Police. This is a pity, since their favorite topics of discussion are tax frauds and overthrowing the government.

These enemies have almost unlimited resources. They always listen in to telephone conversations between Alice and Bob. And these enemies are very sneaky. One of their favorite tricks is to telephone Alice and pretend to be Bob.

Well, you think, so all Alice has to do is listen very carefully to be sure she recognizes Bob's voice. But no. You see Alice has never met Bob. She has no idea what his voice sounds like.

So you see Alice has a whole bunch of problems to face. Oh yes, and there is one more thing I forgot so say - Alice doesn't trust Bob. We don't know why she doesn't trust him, but at some time in the past there has been an incident.

Now most people in Alice's position would give up. Not Alice. She has courage which can only be described as awesome. Against all odds, over a noisy telephone line, tapped by the tax authorities and the secret police, Alice will happily attempt, with someone she doesn't trust, whom she cannot hear clearly, and who is probably someone else, to fiddle her tax returns and to organize a coup d'etat, while at the same time minimizing the cost of the phone call.

A coding theorist is someone who doesn't think Alice is crazy.

Information

The other thing coding theorists are concerned with is information. Nothing else is like information. Information is very peculiar stuff. It can both be created and destroyed. You can steal it without removing it. You can often get some just by guessing. Yet it can have great value. It can be bought and sold.

One type of information is called Money.

There are people who refuse to concede that money can be created and destroyed. They spend their entire lives altering records and making adjustments to ensure that every time a bit of money leaves some place, an equal bit seems to appear somewhere else. These people are called accountants.

Source, channel and secrecy coding

Coding theory, like Gaul, is divided into three parts, called source coding, channel coding and secrecy coding.

Source coding

First I'll tell you about source coding. Source coding is what Alice uses to save money on her telephone bills. It is usually used for data compression, in other words, to make messages shorter.

There is a story about a student of information theory on his first day at college. He had entered a strange, bizarre world. The only sounds were the occasional calling out of a number by one of the professors, followed by laughter. One professor would say '52', there would be a short pause then peals of laughter. Someone else says '713', same thing, everyone falls down laughing.

"What's going on here?" he asked his tutor.

"We're telling jokes," said his tutor.

"Telling jokes?"

"Yes, you see, we've all worked here so long we know each other's jokes. There are a thousand of them. So, being information theorists we applied data compression. We just assigned them all numbers, 0 through 999. It saves a lot of time and effort. Would you like to try? Just say any number 0 to 999..."

He wasn't fully convinced. But he tried. Very quietly he whispered "477".

Hardly a murmur.

He looked at his tutor. "What's wrong?" he said. "Try again," says the tutor.

So he does. "318" - same again, not a thing, hardly a murmur.

"Something's wrong," he says.

"Well," says the tutor, "it's like this - it's not so much the joke as the way you tell it!"

There is a curious sequel to this story. This student eventually succeeded by accident in the most dramatic and unexpected way. He called out a number outside the range 0 to 999. "Minus 105," he said.

At first there was stunned amazement, then first one professor laughed, then another then another, till they were all rolling about holding their sides.

None of them had heard that one before.

Channel coding

Next we come to channel coding. Channel coding is what Alice uses to overcome the noise and interference on the line. Most people have a natural instinct for channel coding. What they do is to spell out important words. This adds redundancy and enables the listener to cross check. If part of the message is lost the missing bit can be reconstructed from the remaining part.

Many organizations such as the military, the aviation community, the Police and so on use a standard phonetic alphabet specially designed for this purpose. It goes Alpha, Bravo, Charlie, Delta, Echo, Foxtrot, etc. So one says "Mike" and "November", which is much clearer than saying "M" and "N" which are easily confused otherwise.

Alice uses this to explain to Bob that her husband Michael is getting suspicious of her stock option dealing.

"I have to tell you about Mike," she says. But Bob hears "I XXve to tell u XXt Xxike".

"What's that again?" says Bob. "I have to tell you about Mike," says Alice.

"Didn't get the last word Alice," says Bob, "can you spell it out?"

"Mike India Kilo Echo" says Alice.

"Got India Kilo Echo, what was the first word?" says Bob.

"Mike"

"Can you spell that?"

"Mike India Kilo Echo" etc.

Actually there have been lots of other phonetic alphabets. The predecessor to the International Phonetic Alphabet went Able, Baker, Charlie...

Then there are those based on names of countries:- Africa, Brazil, Chile, Denmark, England, France, Greenland, Holland, India, Japan, Khazakistan, Lithuania, Morocco, Niger, Oman, Papua, Qatar, Russia, Spain, Tanzania, Uruguay, Venezuela, Westphalia, Yemen, Xanadu, Zambia.

My personal favorite is this:

- A for 'Orses
- B for Mutton
- C for Yourself
- D for Mation
- E for Brick
- F for Vescence
- G for Police
- H for Consent
- I for Lutin
- J for Orange
- K for Teria
- L for Leather
- M for Sis
- N for Mation
- O for A Muse of Fire
- P for Ate
- Q for A Song
- S for Something Else
- T for Two
- U for Mism
- V for La France
- W for Mism
- X for Breakfast
- Y for Lover
- Z (zee) for yourself

Secrecy coding

Finally we come to Secrecy Coding, or Cryptography. Secrecy Coding is what Alice uses to try to stop the tax authorities and the secret police understanding her telephone conversations.

Now cryptographers are very peculiar people. They have very devious minds. Sometimes they encrypt jokes. Security agencies call these "Covert Jokes". People who make them are CryptoLaffers.

An intelligible joke in its raw form is called the Plainjoke, and after encryption is called the Cipherjoke or Cryptojoke. Cipherjokes are intelligible of course only after Decryption, or as some people call it, after explanation.

There are three kinds of attack on an unintelligible cryptojoke according to the Jokeanalyst's resources. Firstly there is the Cipherjoke-only attack in which the Jokeanalyst is assumed to have unlimited amounts of material which is alleged to be funny.

Secondly and more powerfully there is the Known Plainjoke Attack in which he is given examples of jokes together with their explanations.

But most powerful of all is the Chosen Plainjoke Attack where he gets to ask the Cryptolaffer to explain WHY the joke is funny.

Feeble jokes are usually encrypted using only a very simple cipher, like changing the punch line. This is called the DEFLECTED ENDING SYSTEM or DES.

Very good jokes, the comprehension of which by outsiders could constitute a threat to national security, are encrypted much more securely, usually by completely changing the scenario, the plot and the conclusion. This is the PARTICULARLY KLEVER COVERUP or PKC. The best known PKC RESISTS SERIOUS ATTACK and is therefore called the RSA.

As a corollary of course, it follows that only very gifted, intelligent people can truly appreciate a funny speech.

Standardisation

Since it is difficult to design a good cipher, and since the apparatus is very expensive, a lot of work has been done recently to try to standardize on them. Even as I speak the International Standards Organization is meeting to decide on this very issue. Since there is a lot of confusion on this point I have been asked to make the position clear. The purpose of language is to convey information. This only works if both sender and receiver of information both use the same system. In other words language only works precisely because it is standardized.

The purpose of cryptography on the other hand is to make the message unintelligible except to one person. In other words cryptography only works precisely because it is NOT standardized.So what they do is to make most of the cipher standardized, and to concentrate the non-standardization into one part called the key.

So far so good. But of course the key, the non-standardized part, must be nonstandard in only standardized ways. And also key management must conform to certain standards. In other words standards are being formulated whereby the nonstandard parts, which must conform to certain standards of non-standardization, are also to be handled only in a standardized nonstandard way in order to standardize on the overall non-standardization.

I hope this makes the position clear.

Weak keys

Many ciphers have certain bad keys. If you use one of them the cipher is easily broken. For instance all-zeros is a weak key for the DES. There has been a lot of research done into searching for weak keys. Over the years more and more weak keys have been found till now one has to be quite careful to avoid them.

Perhaps it would be a better idea if we looked for strong keys. In fact, why not look for THE STRONGEST POSSIBLE KEY.

Then we could all standardize on it.

Processing delay

Coding theory is not without its problems. The introduction of source coding, channel coding and secrecy coding often introduces something called PROCESSING DELAY. This is the delay caused by the time it takes to do all this coding and decoding. These delays can be enormous.

History gives us instances when this delay has changed the course of world events. There is a recorded case of a two-word military signal which suffered a processing delay of 150 years. The message, deciphered at the Pentagon in 1972, simply read "Send Reinforcements". It was sent on 1830 from Little Bighorn by General Custer.

Consider the message: "Return home at once, trip cancelled." and think of the effect on world events if it had been decoded in time. It was sent in 1492 by Isobella of Spain to Christopher Columbus.

But these delays are nothing in comparison with the next example. We are told by Suetonius that Julius Caesar communicated with the Orator Cicero in a cipher in which 'A' was sent as 'B', 'B' as 'C' and so on. If you apply this cipher to HAL - the computer in the Stanley Kubrick movie: 2001 - you get IBM. Some correspondence from Julius Caesar to Cicero in this complex cipher have finally been deciphered by GCHQ and will be published in the June edition of Cryptologia. Their contents paint a disturbingly different picture of the world from Caesar's official dispatches to Rome in De Bello Gallico.

I am privileged to have an advance copy, from which I will read you an extract.

> *"Alexandria, April 14th 48 BC (think about it)*
>
> *Dear Marcus Tullius*
>
> *Thank the Gods you and I have a secure cipher. I would not care to have our messages read by my enemies. Frankly I don't trust most of the Senate.*
>
> *Take Mark Anthony. Would you trust him? He's so incompetent he couldn't organize a libation at an orgy.*
>
> *Take Gaius Brutus. Would you buy a used chariot from this man? I think he's plotting behind my back. Sometimes he scares the toga off me.*
>
> *And as for the Gauls. What a bunch of morons. I thought all their problems would be solved when we formed the GEC -the Gallic Economic Community. But what happens? We guarantee minimum prices on food exports, the so called "Green Denarius". We provide subsidies on cheap labor saving gadgets - like slaves. Then what happens? We get a run on the Denarius. Inflation runs at record levels. And they squander our subsidies on gross overproduction of wine. We have to sell it off cheap to the Barbarians to maintain the price level within the GEC.*
>
> *I'm fed up with the whole business. When I get back to Rome I'll retire. I have it all planned. I lied about the size of Gaul in my official dispatches. I've found the most divine little spot for my retirement which I'm keeping quiet about. I'm not having those Senators getting their grubby hands on it. And I've taken steps to make sure they never can. So for your ears alone Marcus Tullius, I have my special, secret retirement place all organized. It doesn't appear on any map because I authorize the maps.*
>
> *Officially it doesn't exist. So it can't be found or taxed. I've managed to conceal a whole extra part of Gaul!*
>
> *So forget De Bello Gallico. The reality is Gaul is divided into FOUR parts."*

The modern world

Well that ends the instant course on coding theory. I would like to finish with a few words on the impact that information technology is having on our everyday lives.

Science has marched ahead so fast that we take for granted the most incredible technological developments. Magnetrons, which were a closely guarded secret during the 1939-45 war are now part of every microwave cooker. And made in Japan. When I was a child, space travel was science fiction. Yet today, advance is so rapid that even the astronauts who set foot on the moon in 1969 had never seen a digital watch. Nor a pocket calculator.

Pocket calculators! Now there's something. They're so complicated! I have a calculator which has sines, cosines, tangents, logarithms, hyperbolic functions and multiple nested parentheses. You can program it in Fortran, Algol, Basic, Pascal, Forth, Fifth and Sixth, ADA and Carruthers. It will factorize primes for you. At present it's working on the Halting Problem.

It translates from one language to another. From German to Spanish. From Macedonian to Esperanto. From Cantonese to Greek. Or from American to English.

It is, in fact, a multiprocessor system. There are 22 Transputers in there. Sometimes they organize a game of football between them.

It has a full color, wraparound wide screen, liquid crystal, three-dimensional holographic display. It's called HoloChromaCinePhotoRamaScope.

Its audio facilities include Dolby Digital Decaphonic surround sound. On the way here I watched "The Labyrinth" on it.

It also has synthetic speech and a voice recognition system. I often talk to it. I tell it my problems. Sometimes it psychoanalyses me. It has me figured as paranoid. But that's just because it keeps getting at me. But don't get me wrong - it can be very user friendly. In fact you can program precisely HOW user friendly you want it is to be on a scale from ONE to TEN.

On a setting of ONE it won't even interrupt a football game to answer you. But on a setting of TEN it's so friendly that on a cold day it pre-heats its pushbuttons.

But no matter who smart it SEEMS, deep down inside it's just a dumb old computer.

One time I got really mad at it. Like all computers, it knew precisely what I wanted it to do. It knew exactly what I MEANT. So why does it have to go and DO what I SAID?

How do you get even with a dumb machine like that?

First I tried slapping it around a little. I pushed its buttons a bit hard. I threatened it. "How would you like a busted display" I said.

But it did no good. It just said "I am virtually unbreakable - and I'm not going to take any notice till you enter the data nicely, like you used to do."

Whatever I did it always seemed to win.

I decided to have a man-to-man talk with it. So I sat it down and said to it "Who's the boss here, you or me?"

No reply.

Again I ask "Who's the boss, you or me? Go on, answer me!"

"I'm thinking, I'm thinking," it said.

So I hit it. Hard. Too hard. I cracked its case.

At first I thought that was the limit of the damage. But then little things started to go wrong. At first there was nothing definite. Nothing you could put your finger on. Just little things like stuttering. It just didn't sound quite the same. Its voice seemed to lack its former confidence.

Then once I caught it making an arithmetic mistake. Of course I didn't mention it. But you could tell it knew. Its self image was shot to pieces.

Saddest of all, it forgot our anniversary - of the day I bought it. In the past this had been a special time for us.

I just couldn't bear it any longer. One evening I tucked it up snugly in its case, lit candles, played a record which was popular when we first met, and sat down beside it.

"Where did we go wrong?" I said. But it had it pride. It wasn't about to weaken in front of a non-machine.

"Wrong? Nothing is wrong," it said. "Just insufficient data."

But underneath you could tell it was hurt.

From there it was a rapid downhill slide.

Now it just mutters to itself. It can only do very simple calculations on small numbers.

Finally came the ultimate indignity. It lost control. It leaked electrolyte all over its case.

I felt so bad about it. My other gadgets weren't happy about it either. They all came out in sympathy for the calculator. My watch gave me a bad time. My power tools keep blowing fuses.

Then one night last week I was driving my car back from London when suddenly the engine stopped all by itself on this lonely country road.

I tried to get out but the solenoids were inhibited by the central locking computer. Suddenly the air conditioner came on and started to blow out freezing cold air. It made a noise like wind whistling through the trees. Then this creepy music came from the loudspeaker. The sort of music they play in movies when the hero is lost in a dark forest.

I got scared. The cold, the wind and the weird music got to me. Then it started to speak.

"You're the guy who beats up pocket calculators!"