WE ARE ALL CODEBREAKERS

We all crack ciphers, we all break codes--we are all codebreakers. Codebreaking is a natural ability all humans have.

We promote the use of our arms and legs--in sports, for example; so we should promote the use of our codebreaking ability. And just like the use of our arms and legs, it will be the highest travesty for anyone to suppress it.

Since we are all codebreakers, the things I have to say in these notes are likely to have been known to my audience already. In a way I am just reminding them of what they already know.

Things we already know are often tangled up with other things we already know, creating confusion and indecision. In these notes I will be doing a bit of disentangling when I think it is helpful.

Codebreakers sometimes do not use their ability wisely, the reason why some people are turned off by codebreaking.

A cipher is a kind of obstruction--like a wall or a vault. We put this obstruction, this wall, around things we want to keep secret, so that intruders cannot get at them. But sometimes this wall can be broken down so that what was once secret is secret no longer.

There are things we have all the rights in the world to keep to ourselves. When people do not respect our privacy; when they break into our houses or our ciphers to steal them; we have good reasons not to look upon them kindly.

Codebreakers do not break into houses, they do not break into vaults, they just crack the ciphers and codes we use. They hack into them and thereby take from us what is not theirs. Codebreakers do not have a good reputation.

Every coin has two sides. What's on the other?

The other side is seldom noticed. One example …

We do not build all the walls in the world; some walls are naturally there. We each live within our own skin. My brain is not your brain. My mind is not your mind. There is a wall around each of us, naturally--a wall around each individual.

But we want to break down this wall! No one is an island; we are social animals; we want to live in the company of other people; we want to reach out to them.

So here we have a wall and we want to break it down. How have we fared? Success? Failure? Full success? Complete failure?

Somewhere in between, it's safe to say. Some of the wall is still there; we are still working at it; we want to continue working at; it is one of the most worthwhile things to do.

How did we break down this wall? What makes it possible for us to reach out to others?

Language. Language has to be one of the things that makes the breaking down of this wall possible. With language we can talk to our fellow human beings, we can converse with them, engage in dialogue, chit chat, …

We have a wall we want to break down. To break down this wall we need language. How do we come to have language? How does each one of us come to have at least one language

with which we can communicate with our fellow human beings so that we can break down these walls that are naturally there between us?

How else except by acting as codebreakers.

We are born codebreakers.

What do codebreakers do?

They turn gobbledygook into meaningful communication. They do so on their own! Without being shown how. Some people know how: those using the cipher. When you have the cipher you can easily turn plain language into gobbledygook, and back again. But codebreakers do not have the cipher; they have only gobbledygook; that's why they have to 'break' the cipher.

Cracking a cipher, breaking a code, is often considered a violent act. Gobbledygook is mess, chaotic mess, big big chaotic mess. Making sense of it is like wrenching order out of chaos. How can you wrench order out of chaos without using force? God can do it; but humans?!

The common impression that codebreaking is violent is another reason why some people avoid the subject when they can.

In the Middle Ages people who could crack ciphers ran the risk of being burnt at the stake. How else could they do it except by enlisting the help of the Devil? The term The Black Art dated from that time. A cipher office where people were engaged in breaking codes was referred to as a Black Chamber.

Violent or not, breaking a cipher is not easy. But when we learned our first language we managed it very well, thank you very much. It took us a few months, but after that we speak just like the natives. What was formerly gobbledygook is gobbledygook no longer.

A child has no concept of a cipher. You can't teach a child a cipher so that they can translate gobbledygook into plain language. A child hears gobbledygook and speaks gobbledygook--to begin with. A few months later they hear like a native and speak like a native. They go directly from gobbledygook to plain language. No cipher. They are just like codebreakers. They are codebreakers. We all are.

Does the child have help from other people? Their parents, for example? People around them?

Of course they have; but they all speak gobbledygook. And they act funny, nodding their heads and pointing fingers.

We are all codebreakers. We are codebreakers from the day we are born. Codebreaking gives us our first language. With language we are able to grow both mentally and intellectually and in the process become part of the human community. Whatever contributions we can make to this community afterwards comes from the fact that we are codebreakers. That we are codebreakers should be celebrated and not decried. Some codebreakers steal; they break down walls illegitimately. But even they, when they are not stealing, participate in the society of codebreakers. Human society is a society of codebreakers.

Since we are all codebreakers it is important that we understand how we do it and why it can be done.

Things humans don't know yet no God can teach them. For it includes who God is. Codebreakers carry out their tasks on their own, without being told by those who already know. Thus when humans want to discover new knowledge they can do nothing else except act like codebreakers, which they are.

Children play with ciphers--both in creating them and in breaking them. Since even children can crack ciphers the basic ideas behind cryptography cannot be all that complicated. As we will see breaking codes is nothing more than 'putting two and two together'.

Putting two and two together is a common activity. Codebreakers do it, detectives do it, scientists do it.

Children, when they start out playing with ciphers, play with simple ciphers. But some do not stop at that; they go on to more and more complicated ciphers, ciphers which are difficult to crack. But whether easy or difficult the basic ideas behind cracking ciphers are always the same.

Cracking ciphers is a matter of putting two and two together. How to put two and two together? Why can it be done? What do we get when we put two and two together? Do we get something we already know? Or something new, something no one has known before?

Scientists discover things nobody has known before. Does this come from putting two and two together? Does putting two and two together have this capability, the capability of producing new knowledge? And if it does, why? Or as some would say, how come?

Codebreaking is possible--since we've all done it at least once, when we learn our first language. Why is it possible?

It is possible because there is a method. I shall describe this method. Readers will recognize it as something they already know.

This set of notes is superfluous. Why tell anybody something they already know? Since we have all broken ciphers, we know the method used. Why describe a method to people who already know?

Most of us can ride a bicycle. How do you ride a bicycle? What do you do?

You paddle? You lean to one side, you lean to the other, and you paddle some more? It is not easy to describe how we ride a bicycle.

And, miracle of miracles, why don't we fall down?!

Things we know we sometimes forget. It is useful that we remind ourselves from time to time of things we already know.

Much can be gained in reviewing past knowledge. Our understanding is never perfect. Given a second chance to look at what we already know, we may discover things that have escaped our attention in the past.

Using pen and paper we can break ciphers. We do not need a lab like scientists; nor a dead body as in the case of detectives. Whatever goes on when we are breaking a code does so in front of us or in our heads. Studying how we crack ciphers is an economical way of finding out how people put two and two together.

Since we are all codebreakers already before meeting on these pages, I am not going to teach you how to crack ciphers. Books on cracking ciphers are easily available.

Books teaching you how to crack ciphers will show you the different kinds of ciphers there are, how they work, and how they can be broken. You will not find that kind of material in these notes. Instead we will be talking about the common sorts of steps we take when cracking ciphers, steps like making assumptions, looking for clues, and so on. We will talk about these steps, ask questions about them, and see what answers we can give--all in the hope that we can be clearer about what we are doing when cracking ciphers and when putting two and two together. I said ‘clearer about’ because, as I’ve said before, in many ways most of us know about these sorts of things already. Here we are just sorting them out and see where they lead.

We will not teach readers how to crack ciphers. Still, it will be useful to have an example of a cipher and then an example of cracking a cipher. Examples help in reminding us of things we already know..

An example of a cipher.

We can construct a simple cipher by replacing the ordinary alphabet with one of our own choosing.

Ordinary alphabet: A B C D E … X Y Z
Cipher alphabet: T K Y M F… R N E
Using this cipher the word BAD will come out as KTM.

Using a cipher we can translate a message in plain language into one that will make no sense to those who don’t know the cipher. The message in plain language is called the

plaintext. After it has been enciphered it becomes the ciphertext. In the present example BAD is the plaintext and KTM is the ciphertext.

For good reason the cipher that we have constructed is called a substitution cipher. The regular alphabet is substituted by a different alphabet.

To recover the plaintext from a ciphertext we usually need the cipher. When you don't have the cipher in your possession, can you still recover the plaintext from a ciphertext?

Sometimes it can be done. It will require some exertion, but sometimes it can be done. The process is called cracking a cipher or, to use the technical term, cryptanalysis.

In the past, once in a while a person would come along and claimed that they could break any cipher (Edgar Allan Poe was one of them). There are fewer of them now. It has now been proven mathematically that some ciphers are unbreakable.

Unbreakable ciphers have been in use for centuries. One of them is called the One Time Pad. You find it mentioned from time to time in spy stories.

Some ciphers are breakable in theory but unbreakable in practice. Breaking a cipher takes time. When the time required is, say, a few thousand years even when using the fastest computer, no one would bother.

Why are some ciphers breakable? And some, unbreakable? Why do we bother with breakable ciphers? Why not use unbreakable ciphers exclusively?

Unbreakable ciphers are 'clumsy'. They cannot be entrusted to memory. If you write them down, they become a give-away. Also they could be lost, or stolen.

That some ciphers can be broken is counterintuitive. You need the cipher to encipher and decipher. Why all of a sudden you can dispense with the cipher and obtain the plaintext from the ciphertext without it?

To this day there are people who do not believe that putting two and two together will get you anywhere. Whatever story you produce at the end is made up, they say, just as Conan Doyle makes up the stories about Sherlock Holmes.

Why did Conan Doyle create the character Sherlock Holmes?

Part of his intention was to promote the use of the scientific method in crime detection. The character was patterned after one of his professors at medical school, a man by the name of Joseph Bell, famous as an expert diagnostician.

Can ciphers be broken?

Let's have an actual case. Let's have a secret message and see if, after breaking it, the result is made up.

Suppose we have found the following on a crumpled piece of paper in a waste basket.

```
SBR SBCTU DBCKERVS FCGG WTTCXR SFH FRRJD YTHE SHUWI
```

What should we do?

We could throw the piece of paper back in the waste basket and go on our usual way.

Or we could say to ourselves, maybe here we have a secret message; let's see if we can break it.

Do you know for sure there is a secret message hidden in the scribbling?

Of course not! But nothing ventured nothing gained. If we find a message, then there is a message. If not, then we don't know.

But wait! Are you sure you know what you are doing? You are here looking for something you don't know. But if you don't know it, how would you know you have found it even when you think you have?

Suppose I've lost my glasses. When I've found it, I know I have because I know what my glasses look like. I know my glasses, so I can look for it. But here you are looking for a secret message. Secret because you don't know it. If you know it, it is no longer secret. But how can you look for something you don't know. How will you know that you have found the secret message even if you have?

This used to puzzle Plato. It is usually referred to as the Meno Paradox, since it appears in the dialogue *Meno*.

SBR SBCTU DBCKERVS FCGG WTTCXR SFH FRRJD YTHE SHUWI

How are we to crack this cipher? Where should we start?

Even if you have never broken a cipher before, after you have examined the cryptogram, you are likely to be saying to yourself, these groups of letters with spaces in between--what are they? Words? Maybe. And SB … SB. Twice! SB = TH? What about R? E?

Now this is the typical sorts of thing we do in this kind of situation. We are trying to put two and two together. That is, we look for clues and attempt to find out what they mean.

There is often more than one answer to a clue. So when we follow clues it is not unusual for us to engage in a bit of trial and error.

The 'bit' could vary from two to some large number. Before the invention of computers we don't like the large number to be too large. If it is too large we may not have time to finish the trials. But with the invention of the computer, large can really be large. Thousands? Millions? It all depends on the computer power available.

The first computer invented was for the purpose of cracking German ciphers during the Second World War. it was called Colossus.

We rely on trial when following clues.

By following clues--and relying on trial and error--readers should try to crack this cipher on their own, to see for themselves that it can be done. They should do this before continuing reading.

Assuming readers have made some attempt in cracking our simple cipher, we now resume.

In cracking a cipher there is sometimes more than one route to the same final result. This is true with our present cipher.

But suppose in one instance in cracking our cipher we reach the following *partial* result.

```
THE THI?? ?HI??E?T WILL ???I?E TW? WEE?? ???? T????
```

What has happened?

Holy mackerel, new clues! New clues have appeared!

Look at the fourth word from the end: TW?. It certainly is a clue, and a very good one. But it was not there at the beginning.

Neither was WEE??.

In putting two and two together we like clues. The more clues we have, the better. But not all the clues are detectable right from the beginning. Some appear only along the way, after we have responded to the initial clues. At this point in our cryptanalysis we have developed so many new clues that we can easily see our way to the end. Gives you a nice feeling; doesn't it?

Question:

When we have new clues, what does the fact that we have them tell us about what we have done up to that stage?

Answer (which everyone is likely to be able to give since we are all codebreakers):

If we have new clues appearing, it means what we have done so far is likely to be right. We have taken many steps to reach these new clues. If the earlier steps were wrong, new clues could not appear.

What are clues?

Why are clues so important? What are they?

Look again at our cryptogram:

```
SBR SBCTU DBCKERVS FCGG WTTCXR SFH FRRJD YTHE SHUWI
```

Here we have a string of symbols that makes no sense. But we suspect there is a message hidden behind it. We want to know this message. So we look for clues. What else can we do?

Why are clues important?

Because they lead us to things hidden, things that we want to know despite the fact that they are hidden.

How do they do that? What gives clues this ability? We think SBR is a clue. It stands for THE. We see SBR. We don't see THE. Why do we say it nevertheless stands for THE?

We see SB twice, both at the beginning of a word. Many English words start with TH. So SB could be TH.

What then is R?

Try E. English sentences often start with THE. So SBR is THE.

The explanation of the clue SBR makes reference to the English language, to some characteristics this language is known to have. Different languages have different characteristics. If you are familiar with the characteristics of a language, you can detect clues coming from that language.

Why is it that different languages have different characteristics?

This is because different languages have different structures. Every language has its own structure. When structure is different, characteristics are different.

A language is not a random collection of symbols. We do not take a fistful of letters, throw it on the table, and thereby create a language. A language has a *structure*. In the English language there are rules governing how letters are put together to form words, and how words are put together to form sentences. Because a language has a structure it has certain characteristics. It is a characteristic of the English language that many of its words begin with TH.

So, what are clue?

Clues are nothing more than the characteristics of structures, disguised. It is a characteristic of the English language that many of its words begin with TH. In our cryptogram we do not see TH at the beginning of any word, but we see SB at the beginning of two. SB, we say, could be TH in disguise.

Language has structure. But components of a language also have structure. A sentence has structure. Also a word. This is a common thing: there are often structures within structures.

If you have a three-letter word and the first two are TW, what could the third be?

A thought experiment:

Encipher a random string of symbols. What do you get?

Another random string of symbols.

Can you recover the original random string from this second random string without being given the cipher? That is, can you break the second string?

You cannot--because there are no clues. A random string has no structure (that’s why we call it random). No structure, no clue.

Language has structure. A cipher also has structure. In our SBR example S always stands for T. A plaintext letter is always substituted by the same ciphertext letter.

If you have a meaningful communication as plaintext, and by enciphering it, you destroy all the structures present in it, you will have produced a cryptogram that is unbreakable. The cryptogram will appear as a random string. Random strings contain no clues whatsoever.

But where can you find a cipher which will do this, a cipher that destroys all the structure in the plaintext? All ciphers have structures. Your original plaintext is meaningful and therefore has structure. Applying any cipher to a structured plaintext will produce a cryptogram that contains clues.

How can you turn a meaningful communication into a random string of symbols and back again using a cipher? It seems impossible. All ciphers have structures

But it is not impossible; there are unbreakable ciphers. The trick is, you don't use *a* cipher. You use a *series* of ciphers. A random series.

Important point: You use the same random series both for encipherment and decipherment. You don't shuffle the series after encipherment. If you do, you will not be able to recover the original plaintext.

So this is what you do to generate an unbreakable cryptogram from a meaningful plaintext. You take your random series of ciphers. You encipher the first letter using the first cipher in this series; the second letter, the second cipher; and so on. The result? A random string of symbols.

Using the same random series (of ciphers) in reverse you get back your original message.

An unbreakable cipher is actually of series of ciphers. A random series.

To break a cipher you need clues. Clues are the characteristics of structures. If you obliterate structure you obliterate clues. An unbreakable cipher is one that obliterates structure in the process of encipherment and restores it during decipherment.

Interim Evaluation

In cracking ciphers we do not have to wait till the end to find out whether our results are right. From time to time we can provide Interim evaluations. We do this by watching out for new clues. New clues not only make further progress possible, they also tell us we have been doing things right, that we are on the right track.

Clues are the characteristics of structures, disguised. The more of the disguise you can removed, the more of the structure is revealed.

At the beginning of an investigation we usually do not have all the clues we need. But clues lead to new clues. However, they can do so only when they have been properly deciphered. Thus when new clues appear we know what we have done are likely to be right. The more generations of new clues, the more likely to be right we are.

How do we develop new clues?

We do so by applying what we have learnt from previous clues to the evidence / ciphertext. A three-letter word in which two of the letters have been deciphered as a result of previous clues *is* a new clue.

This kind of retrospective evaluation we carry out when putting two and two together covers a lot of territory. New clues cannot appear if we have made *any* serious mistakes *anywhere* in the investigation up to that point. Clues are not the results of chance. Even less are generations of of new clues.

False clues sometimes appear by chance. But false clues peter out.

In looking for lost items like a pair of glasses, we don't look for half of the pair first and then the other half later on; we look for the whole thing, all at once. In following clues we are looking for something. But we don't find this 'something' all at once. We find parts and then we find more. And as we move ahead in this journey of discovery, we know whether we are on the right track and whether we are heading in the right direction. We know because this 'something' we are looking for are structures.

There is an art in following clues. But following clues is also at the same time a science. Following clues is both an art and a science. As a science it depends on some basic ideas. From these basic ideas we can derive general rules, general directives. These basic ideas also give the process (of following clues) some distinctive characteristics which people often notice. Interim Evaluation is one of these. When new clues appear, old clues are likely to have been correctly interpreted.

The Art and Science of Following Clues should have a more convenient name. I propose Theseology. Theseus went into the Maze to kill the Minotaur. To ensure that he could come out again he unwound a spool of thread as he went in. The thread marks the way in and also the way out, like a cipher--which turns plaintext into gobbledygook and back again.

‘Theseology’ sounds too much like ‘theology’. But maybe in time we will get used to it.

Can a person with just one or a few clues, and not developing any new ones, discover so much that they need a whole book to record the results?

It is theseologically impossible.

But that is what conspiracy theorists do. They weave an elaborate theory around a few facts (which they sometimes even call ‘clues’) and then keep on adding more and more details, all constructed out of thin air.

They are not theseologizing; they are just making things up.

Theseology is both an art and a science. It requires ingenuity to detect clues and to interpret them. It is a science when it comes to the evaluation of results. That we can have interim evaluation belongs to the science part of theseology. This is also the part of theseology which allows Sherlock Holmes to say, ‘Elementary, Watson!’

Interim evaluation is an interesting characteristic of the theseological process. This kind of evaluation depends on new clues appearing after old clues have been interpreted. Old clues lead to new clues …

There are feedback loops when we are following clues!

And it is *positive* feedback. Clues lead to *more* clues. Success leads to *more* success. No wonder we learn our first language so fast: we are our own teachers!

And when you are your own teacher, why hire one? Or ask God?

Learn by immersion! That should be your slogan, and mine, and everybody's.

When Sherlock Holmes is trying to solve a crime, he replays it over and over in his head. He tries to think like the criminal. He immerses himself in the crime. It requires great concentration. That's when he takes out his pipe.

How did Kekule discover the structure of the benzene molecule?

The idea that the benzene molecule is in the form of a ring came to him in a dream--of a snake swallowing its own tail.

When you are immersed in your work your mind doesn't rest even when you are dreaming.

Discovery is hard. But evaluation is easy. Which is to say, they occur together.

Clues lead to more clues. Scientific discoveries make possible other scientific discoveries. Kekule dreamt the right dream.

Small Steps Principle

Clues lead us to the things we want to know but at the moment do not know. This they do in small steps, never big ones. I call this the Small Steps Principle.

When we have a ten-letter word and one letter is missing, we can fill it in. But if only the first and last letters are known we have no way of knowing the remaining eight without more clues.

The Small Steps Principle is not usually spelt out but is well reflected in practice. In following clues we are forbidden to take huge leaps and we don't jump to conclusions.

Every person's vocabulary is limited. From time to time we come across words already in use but not familiar to us. When this happens we don't alway run to the dictionary. We can figure out what the word means from context. Context acts as the clue.

How are new words invented?

We use words in real or imagined situations. In doing so we sometimes come across lexical gaps that can't be filled with existing words, so we invent a new one.

Language does not stop growing. It evolves as society evolves. We can keep up with changes in language because we are codebreakers. We are born codebreakers. We do not stop being codebreakers.

The Small Steps Principle makes it possible for us to use approximations in investigations. A clue is a small gap in our knowledge. We can close this small gap completely in one single step or we can fill it partially with an approximation, leaving a tiny gap to be bridged later on.

Clever use of approximations makes some investigations easier. An atom is not exactly a miniature solar system. No matter. If it is close enough, we can still find out a lot. After that we go native.

Evidence and Feedback

In cracking our SBR cipher the cryptogram is long enough to provide us with enough clues so that we can recover the cleartext. If it had been shorter our task at cryptanalysis would have to be cut short.

One simple way of making a cipher unbreakable is to send only short messages--and not use the same cipher a second time. This is the principle behind the One Time Pad.

It is well known that in following clues, if we do not have any evidence, or not enough evidence, nothing can be found. In cryptanalysis the ciphertext (intercept) is the evidence. The more evidence we have the easier it is to crack the cipher.

Without saying, by evidence we mean of course relevant evidence. How do we know; how do we recognize; relevant evidence? Evidence does not come to us and introduce themselves. Yes some might; but not all.

In our SBR example, although we have recovered the cleartext, we have only reconstituted part of the cipher.

Suppose we now have a new intercept. Will it help us to work out the rest of the cipher?

It will only if it comes from the same cipher.

How do we know whether the new intercept is from the same cipher?

We apply the part of the cipher we already know to this new intercept to see if it can be partially deciphered. If it can, it is from the same cipher.

In cracking a cipher success leads to more success: clues correctly interpreted lead to more clues. This is one way feedback works in the theseological process, that is, in the production of clues.

There is a second way in which feedback works, and that is in the collection of relevant evidence, as we have shown above.

Let us make the following equivalences.

Cipher = Theory
Ciphertext = Evidence
Cleartext = Meaning of Evidence

When an investigation is going well we advance on all three fronts. That is, we have a more complete theory, we have more evidence, and of course we know better then what the evidence means. This concurrent motion forward is dependent on feedback. Without feedback the investigation would not go anywhere.

Science advances on three fronts. This round disc in the night sky, which changes shape as the nights go by, is a material sphere--not a body made of some fifth essence; and its motion across the sky follows the laws of physics.

The beginning of an investigation is usually the most difficult. For, to begin you have to assemble a set of assumptions, gather evidence, look for clues, …; you have to do all this while largely in the dark.

But once you have hit upon a few right moves, feedback takes over and the investigation catches on fire.

There are a number of elements we have to get right before an investigation can acquire momentum--for example, the right set of assumptions. This task, while difficult, is made a little easier in that even at this important stage of the investigation, we do not have to get everything exactly right; we do not have to be perfect. When following clues we are allowed to use approximations. So long as the approximations are good enough for the investigation to advance, we have the opportunity to *turn back* and bring these approximations closer to the truth.

So here we have another instance of feedback occurring when we are following clues.

That approximation is permissible applies to evidence, whether late or early in an investigation. Evidence does not have to be perfect. So long as it is good enough for the investigation to advance, it is all that matters.

The evidence in support of John Dalton’s Atomic Theory was quite rough at the time the theory was proposed. But the theory was accepted and chemistry moved on.

Why do we rely so much on our senses when we gather evidence? Certainly it can't be because our senses are perfect.

Our senses are imperfect; they are prone to error; but they have been the objects of our attention for so long that now we have a good idea under what conditions they will produce results good enough for the purpose for which we are using them.

Some objects are so small our eyes can't see them. We put them under a microscope and the images they produce become evidence for some investigation. Why would we allow ourselves to do this?

We allow this to happen because the microscope is constructed according to what we have understood of the properties of light. Past discoveries help in future discoveries by supplying us with instruments--another instance of feedback.

Assumptions

In cracking a cipher we look for clues. But in doing so we would have already made certain assumptions. What kind of clues are we looking for? Clues coming from the English language? If that is the case, it means we are assuming the plaintext is in English. And the cipher--what kind of cipher? Substitution? Letter for letter?

We call these 'assumptions' because we have little evidence for them. In our present case the reasons for them are largely circumstantial. We are communicating in English, we are working at a simple example; so, very likely, the plaintext is in English and the cipher a substitution cipher.

When following clues we always have to make assumptions, consciously or subconsciously. Without them (the conscious part of) the investigation cannot start.

Will we ever know our assumptions are right? Do we have to wait till the end of the investigation to find out?

We should notice once again that we do not have to wait till the end. In following clues if we meet with success after success; if more clues appear after old clues have been interpreted; our results so far are likely to be right.

Results include the assumptions we make at the beginning of the investigation, assumptions that at that time rested on wobbly ground.

What happens if we have made wrong assumption?

If we have made the wrong assumptions we will not get anywhere. In our SBR example try the assumption that the cleartext is in German.

We rely on assumptions to detect clues. German clues do not arise from English messages. The German language has a different structure from English. If by accident a few false clues appear, they will have no offsprings; they will not lead to new clues. Accidents do not compound themselves indefinitely.

In deductive reasoning different premises leads to different conclusions. In following clues, if we start with different assumptions, will we not have different results?

Following clues is not like deductive reasoning. In deductive reasoning from any set of premises you can always draw some conclusion, interesting or dull. When we are following clues wrong assumptions produce no clues. No clues, no results.

Theseology is not Logic. The former studies how we follow clues; the latter, how we reason.

It is true that we reason when we follow clues, but that does not make Theseology a part of Logic. Physicists also reason. No one would say Physics is a part of Logic.

Correcting Mistakes

In cracking ciphers a certain amount of trial and error is unavoidable. Sometimes the amount of trials can be huge. But since we now have computers, so long as the trials can be completed within an acceptable time limit, we will go ahead.

Who makes the trials? Who corrects the errors?

The same people. The codebreakers themselves.

Codebreakers correct their own mistakes, not those who already know.

If you are cracking Hitler's ciphers, Hitler is not going to tell you how well you've done.

How can codebreakers--people who are still in the dark--correct their own mistakes. If you don't know what is right, how do you know what is wrong? If you don't know what is true, how do you know what is false?

How we correct mistakes when following clues depends on what kind of mistakes they are. There are three kinds of mistakes when following clues.

1. Simple
2. Hidden (single)
3. Hidden (multiple)

Simple mistakes are those we can correct in the normal course of an investigation.

A clue is a mall gap in our knowledge. We fill this gap by trying out possibilities one by one, to see if they fit. Suppose we now find one that does the job. We congratulate ourselves and we stop. Did we make any mistake here?

In this example we could have. We could have stopped too early. There could be other possibilities that could also fit.

How do we detect this kind of mistake?

We detect it usually in the normal course of the investigation. In an investigation, constant review is very much a normal part of the process. In reviewing what we have done we could detect mistakes.

How do we correct simple mistakes?

In our example, since the mistake is one of stopping too early, we continue with the trials. If we find there is more than one possibility that could fit the clue, we look for additional clues to see if we can eliminate all of them except one.

When there are only two possibilities to fit a clue and we want to eliminate one of them, we often speak of triangulation. One clue points in one direction, a second clue points in a different direction. Where they intersect, there's your culprit.

In following clues, from time to time we have to sit down and collect our thoughts. What have we done so far? Are there any mistakes?

In an investigation we review what we have done not just once, but over and over again. This is essential. One of the consequences of this constant review is that we can correct mistakes.

Review performs another important function. It familiarizes us with the terrain, making it that much easier for intuition to do its job when it decides to come to our assistance.

Following clues--like playing chess--requires intuition. That is the art part of theseology.

Mistakes we can correct in the normal course of an investigation, I call simple. They are relatively easy to detect and correct. But sometimes mistakes we have made bury themselves so well in the investigation that we don't see them in our normal reviews. But because they are there they can create havoc and confusion. Clues dry up, and ultimately the investigation reaches an impasse.

To correct hidden mistakes we usually assume first there is only one. This is because correcting multiple hidden mistakes is much more difficult.

To correct a single hidden mistake the common practice is to retrace our steps. Since when a hidden mistake is made progress will become impossible, we check our most recent steps

first. If the mistake is there and we can correct it, we should be able to advance again. If we cannot find the mistake there we will have to go back farther and farther, until eventually it is found.

In retracing our steps to correct a hidden mistakes we sometimes may have to go all the way back to the assumptions we made at the beginning of the investigation. If we find the mistake there and have corrected it, we often speak of a ‘revolution’. A change in assumptions gives the investigation a very different hue.

In retracing our steps, how do we know which step is a mistake?

This is usually not an easy task and may include a fair amount of trial-and-error. For, if the mistake were easy to detect we would not have made it in the first place. But since it is causing the impasse, if we can replace the wrong step with the right one we should be able to move forward again.

If there is only one hidden error, by replacing the wrong step with the right one we should be able to move forward in the investigation. But suppose we have made not just one hidden error, but more than one. Suppose also that Step A is one of the wrong steps. Now if this is the case replacing A by the right step will not rejuvenate the investigation (since there are other hidden errors besides Step A).

What do we do then?

Correcting a single hidden error is difficult enough. Correcting multiple hidden errors is even more difficult.

The common way to correct multiple hidden errors is to re-do the whole investigation, or the part of it in which the hidden errors are suspected to have occurred. The hope here is, the same mistakes will not be made a second time.

But what is the likelihood that we will not? If the mistakes were not easy to make we would not have made them in the first place. If we have made them the first time the likelihood is high that we will make them a second time.

What can we do then?

One thing we sometimes do is to call in new blood. Instead of having the same people working on the same investigation a second time, we hand over the investigation to a new group of investigators. The hope here is that this new group will look at the situation in a different way and as a result not make the same mistakes.

When we call in new blood, to better improve our chances we should prevent the new group from knowing what the old group has done. If we do not; if we let the old group brief the new group, for example; the new group might, consciously or unconsciously, approach the investigation more or less in the same way and thus make more or less the same mistakes. Ignorance is not always bliss, but in this case it is.

In following clues it is best if we correct mistakes as soon as we can. Once mistakes have burrowed themselves in an investigation they are hard to unearth.

Investigators and their partners have to be vigilant and outspoken. Once they suspect a mistake has been made, they should speak out.

People who follow clues welcome critics--whether they like them or not.

Method

We as codebreakers have a powerful method in our hands. It enables us to uncover hidden structures on our own, without the help of those who already know. In following this method codebreakers monitor their own progress; they do not have to wait for some end point at which time ‘all will be revealed’. In fact, it does not matter to them whether that end point ever comes.

This method we follow when breaking codes does not have a name. Since we follow clues when breaking codes, I propose we call it the theseological method.

The theseological method is not simple. Its main advice to us is that we should follow clues and develop new clues from old. Once we have gotten this message, the rest of the method follows naturally.

A method assures that the results it leads to are correct. We have a method for doing sums using pen and paper. As long as we follow this method, we know our results are right. After adding 7 to 18 to get 25, we don't have to put down pen and paper and start counting toes and fingers to make sure that 25 is really the right answer.

The same with breaking codes. After cracking Hitler's cipher you don't call him up on the phone and ask, 'Did I get you right, your order to Rommel?'

Some methods are so simple and easy that they are foolproof. Anyone can follow them and get results. The theseological method, the method codebreakers use, is not foolproof. It takes ingenuity to detect clues and figure out what they mean. But so long as we succeed in following it, it produces the right results.

Children learning their first language do not know that they are following the theseological method. This is not surprising. Many things we do we learn simply by doing.

Not know how to ride a bike? Get on one and pedal away! You will fall a few times but ...

Is the theseological method the same as the Scientific Method?

This is a complex question. It should be divided into three.

1. Is Science made possible by a method?

   Yes.

2. Is Science made possible by a New Method discovered at the time of the Scientific Revolution?

   No; no New Method was discovered.

3. What method made Science possible?

> The theseological method (‘follow clues and develop new clues from old’), the method codebreakers had been using long before the Scientific Revolution.

Newton broke codes for Elizabeth I and James II.

When you break codes, one of the first questions you have to answer is, what is the language of the plaintext?

Galileo thinks the Book of Nature is written in the language of mathematics.

Which branch? Geometry? Algebra?

Neither, says Leibniz; instead, binary arithmetic! Which he invented.

It is a common belief that the New Science ushered in by the Scientific Revolution was made possible by a new method. New method, therefore New Science.

Sounds great but false!

The New Science was made possible by an old method, the theseological method. Old method, new science.

Strange but true.

How can it be? If the method is there, should the science not be there as well? Why do we need a revolution to bring in the New Science? What’s the big deal?

The big deal was that the theseological method, although known in practice, had never been applied to the study of nature by mainstream scholars. During the Scientific Revolution the theseological method came into the mainstream. It was the theseological method applied to the study of nature that brought in the New Science.

Scientists applied the theseological method to the study of nature. Sherlock Holmes applied it to crime investigation. All the time of course, codebreakers had been using it.

Reminders and Expansions

‘All truths are easy to understand once they are discovered; the point is to discover them.’

—Galileo Galilei

After they have been shown one example in cracking a cipher, people often ask for more. Cracking ciphers is absorbing … as well as liberating. For once--perhaps even for the first time--one becomes fully aware that one can make discoveries on one’s own.

‘How do you know?’--People often think there is only one way to answer this question, and that is by citing some authority; which of course raises the question how Authority knows.

But there is another way to answer the question. We know by following clues. This answer does not lead to infinite regress.

The authoritarian view of knowledge--that knowledge ultimately depends on authority--has undesirable consequences. For one it leads some to claim that they are the ultimate authorities and thus everyone should obey them.

We learn our first language by ourselves (with encouragement by parents and those around us). This is a good example of individual autonomy. But the autonomy enjoyed by a child does not last long. Once they have learnt a language, there always will be some among their elders who will use the language they have learned to tell them what to do and what to believe.

The theseological method overcomes subjectivity. When we succeed in following this method, we will have uncovered what is objectively true.

When you have broken Hitler’s cipher, whatever you might think of Hitler as a person, the cipher you have broken is indeed the one he is using.

When solving crimes Miss Marple has an advantage over most other people in that she has a good memory of past events, including village gossip. It helps her detect clues.

In preparation to solving a crime Miss Marple does not empty her mind of all preconceived ideas so that she can look at the facts surrounding the case objectively.

Background knowledge helps us detect clues. The wider and deeper this knowledge, the better our chance. Clues are the characteristics of structures; knowledge is knowledge of structures.

How did Miss Marple build up her background knowledge? Why did she know so much about things to which other people would not pay any attention?

She is a curious person. We are all curious--to different degrees and about different things.

And it is good that we are curious. You never know which item in your background knowledge might one day help solve a crime.

But surely you don't build up your background knowledge with the expectation that you will solve a crime one day?

No; we don't pursue knowledge only when we think it is useful. Knowledge has value in itself.

Knowledge for its own sake?

Yes, knowledge for its own sake.

An 'ought' cannot be logically derived from an 'is'. But an 'ought' can be *discovered* by taking small steps when following clues.

Clues are the characteristics of structures. Sometimes the structures we are investigating are not among those we already know. How then can we detect clues in such a situation?

We use our imagination; we create structure after structure until we find one that helps.

It might take a long time ...

Then do it in advance. Let those who enjoy using their imagination exercise their creativity.

Art for art's sake?

Art for art's sake.

And sports for sports' sake.

Et cetera.

Tyrone Lai
September, 2016