

THE NUMBER MYSTERIES –
Presented by Professor Marcus du Sautoy

LECTURE 4: THE CASE OF THE UNCRACKABLE CODE

Broadcast on: 28th December 2006



Part 1

Marcus

Welcome to The Number Mysteries and the case of the uncrackable code. Ever since we've been communicating we've been using codes, but it's during wartime that codes become really important. You don't want your enemy to know what you're going to do next.

Now one of the most sophisticated encoding machines is this one here. It's called the Enigma machine, and it was used by the Germans during the Second World War. They used it to keep their messages secret and they thought this was uncrackable, but mathematicians sitting up in Bletchley Park – just north of London – found a way to crack this code. During this lecture, we're going to try and re-enact this great feat of the mathematicians by challenging a team up at Bletchley Park to break the Enigma code. Now earlier today, Evil Andy over here locked away a load of sweets inside this safe. He's locked it with a combination, and only Evil Andy knows the combination. To make it even doubly secure, he used our Enigma machine to encode the numbers and so it's become an even more scrambled mess. I've found this secret message that he's encoded here, and we're getting it now, sent up to Bletchley Park. This is Daniel Clack and he's sending it by Morse code, to the mathematicians in Bletchley Park, and we're hoping they're going to be able to decode this message. So how are you doing Daniel?

Daniel

It's nearly done, Marcus.

Marcus

Nearly done, OK. There we go, well let's give Daniel a big round of applause for sending our secret message out. Right, now the trouble is that I don't know quite how Evil Andy set up this Enigma machine this morning, when he encoded this message. That's the challenge for the team in Bletchley Park to try and find how Andy encoded this, how was the machine set up when he wrote this message. If the team at Bletchley Park manage to crack this code by the end of the lecture all those sweets are yours. But if they don't do it, then Evil Andy walks off with all the

sweets. Now we've got a web link all the way up to Bletchley Park over here, and we're going to go and meet Tony Sale, whose one of the code crackers at Bletchley Park. Hi Tony, can you hear me?

Tony Hello, good evening.

Marcus Great, now did you manage to get the secret message we sent up by Morse code?

Tony Yes, I did, I've got that, yes.

Marcus OK, so how on earth are you going to find the settings that Andy used on the Enigma machine?

Tony Well we're going to use a reconstruction of the bomb machine. It was invented here in World War Two, which finds the settings for the Enigma machine from the cyber message.

Marcus And how long do you think it's going to take?

Tony Hmm, probably about half an hour.

Marcus Half an hour?

Tony If it works, yes.

Marcus OK, if it all works. Well I've got 400 kids here hoping you're going to be able to crack this code. We've got a hotline here, so please call us when you've cracked it and hopefully we'll make all these kids happy. Good luck.

Tony Right, will do.

Marcus Now in this lecture I want to show you how mathematics has been used to make and break some of the cleverest codes around. And at the end of the lecture I'm going to explain how you can even win a million dollars – not just the sweets in there, but a million dollars – if you can crack some of the mathematics behind some of our modern codes. In fact, there's even a way that you can win this Enigma machine. If you go to our website you'll find out how you can even win this machine here.

Now the Morse code that Daniel was using earlier on to send the message up, consists of a load of dots and dashes; changes the letters into dots and dashes. And this Morse code was created 170 years ago to send messages down telegraph wires. Now you can see the code up here on the screen. So for example, if you look at the top then A is a dot, followed by a dash – so that would be dot-dash. But if you look a bit further down, the E is also a dot and then if you look across T is a dash. So it's very difficult how to tell whether I wanted to send an A, dot-dash, or ET which is also dot-dash. This makes it very difficult to actual interpret the Morse code. Especially for a machine, or say something like a computer trying to read Morse code.

In the 1870s a Frenchman, named Emile Baudot came up with a new code, which was much better and solved this sort of problem. And here is the code. So, this is Emile Baudot's code. Now what you're going to see here he's replaced ever letter by some dots and spaces. He's given every letter the same number of dots and spaces: there are five dots and spaces to represent every letter. So, for example, if I look down here, X is a dot-space-dot-dot-dot. And Y for example, is dot-space-dot-space-dot. Now this is much easier for a computer to read. So, for example, I found some tickertape here, so you can actually print this out on a piece of tape and all the holes then... the dots become holes in the tape and the spaces are left blank. Now I found this lying around on Andy's desk a little bit earlier on, and I am actually hoping, maybe, these are the secret numbers for the combination locks. So, I wonder whether anybody could help me to try and decode the Baudot code that I've got on this tickertape. OK, do you want to come out? Maybe we'll get the secret numbers and we won't need Bletchley Park after all. OK, so, what's your name?

Nick Nick.

Marcus Nick. What we need to do is to feed this inside here – this is a machine that can read all the holes and the spaces and tell us what the message is. I think we put it here and now we need to switch it on. OK, so if you'd like to press that one there, Nick, I think it will start telling us. Here comes the message. Read it up here. OK, can you read? Let's switch this off. What does the message say, is it numbers? No, it's not numbers, can you read that out?

Nick It says, you won't get the chocolates this way, signed Evil Andy.

Marcus

Evil Andy, my God he's messing with us, oh well there we go. It's not the numbers, but Evil Andy messing with us. OK, let's give Nick a big round of applause, for trying to decode. I think we are going to have to rely on Bletchley Park; Evil Andy is just messing with our minds. Well, this idea of using the language of mathematics is actually a major breakthrough in the history of codes. The dots and spaces, or ones and zeros, are easily converted into electrical signals and then these can be sent across the electricity lines and telegraph lines. And it's used in nearly every form of communication devices today. For example, your mobile phone, or when you're watching digital TV or anything like that, iPods and things like that, all the music, the pictures are translated into loads of zeros and ones. So that's how these codes can encode the world around us.

Now you may even be able to spot the code in this. If I show you this, this is Coldplay's recent album. In fact the title of the album is written in Baudot code, this sort of zeros and ones codes. I've got a large version of it over here, which I'm going to try and decode for you. So this is the name of Coldplay's album, they wrote it in Baudot code. So, if I could squeeze in here. OK, so the colours are kind of irrelevant here. Just, if there is a colour, that means we've got a black dot. So, for example, there's colour here that means we've got a black dot. We've got a space here that means there's a space in the Baudot code. So, for example, this first column here represents a letter and here I've got colour-colour-colour, so that's spot-spot-spot. If we look here, this is the first letter in the title is in fact X. If I go to the end here, we have colour-space-colour-space-colour. And if I turn that round, so that's dot-space-dot-space-dot. Remember, that was the Y that I read out earlier. Now I want a volunteer to try and help me to decode the last two, the middle two, columns here. Yes, would you like to come up, sir? And you'd like to go this side of our Baudot code, and yes, let's stand you here. What's your name, sir?

Josh

Josh.

Marcus

Josh, let me give you a hint for the first column here. This is actually a bit like the shift key on a typewriter. If you press the shift key, you get all the interesting characters. So in Baudot if you see dot-dot-space-dot-dot, you know you've pressed the shift key. And if you look on our Baudot code all the things at the top are the interesting letters. So we're going to be looking at those, OK? Now the next one, what you've got to find on our Baudot code is, what's this? This is space-

space-space-dot-dot. So let's translate that one, so can you find space-space-space-dot-dot on our Baudot code?

Josh

O.

Marcus

Right, it's O, but you have to shift up, so shift it up to 9. OK, so we managed to decode Coldplay's album. Coldplay's album is actually called X9Y. OK, we'll let's give Josh a big round of applause. Now, that's kind of intriguing because I guess you were all expecting it to be called X&Y. That's certainly what Coldplay hoped to call their album, but they made a bit of a mistake. They actually called the album X9Y, because if you look at what & was meant to be, it was space-dot-space-dot-dot. In fact, they made a little mistake, they should have put a dot here and they didn't. So something got a little bit of mistake here and they ended up calling their album X9Y, of all things. Well this is one of the problems with Baudot, you see you make a little bit of a mistake, it turns into another message.

So, is there any way you could actually correct that mistake? How could a computer, for example, getting this message, know that actually Coldplay have made a mistake and they wanted to put a dot there? Well this is especially important, for example, if you're sending messages back and forth between satellites. There's a lot of interference on the way and a lot of zeros could get changed into ones, or for example, a message from outer space. If you've got a spacecraft sending a message back, that message can get very scrambled with lots of zeros and ones changing. How could a computer actually correct that? Well, luckily mathematics has found a way to automatically correct some of the small errors that get made on the way. I'm going to just demonstrate this, by using some cards on the floor here. Now these cards, lots of zeros and ones, looks like a message which is sent by a computer. Maybe it's in Baudot or something? It's not actually in Baudot, this is something called an error correcting code. Somehow during transmission, some of the zeros get changed to a one, or vice versa, this code is able to pick up that a mistake has been made. Now I'm going to need a volunteer who's going to be a bit of interference to scramble my message, so would you mind to come up? OK, so you're going to be a little bit of noise on the line, what's your name?

Lauren

Lauren.

Marcus

Lauren, now what I want you to do is you're going to change one of these numbers over, so instead of a one it becomes a zero. So if you look down here, Lauren, it's, on the other side there's a zero, like that. I haven't memorised this, but I'm going to get Evil Andy, could you blindfold me? Ow! We want your chocolates, but anyway he's going to blindfold me. Whilst I'm blindfolded I'm going to turn my back, just change one number over and hopefully I'll be able to detect which number you've changed. So that's the blindfold on. Awh gosh, that's a bit vicious Andy! OK, so when you're ready, you tell me when you've changed a number over, please. Just one number. Right I'm going to remove my blindfold and hopefully I can spot which one you've done. So as I said, I haven't memorised this. OK, let's see. I'm beginning to get a feel for it. I think that you changed this number here. OK, pretty good. So was that magic? Yeah, thank you, thank you.

So how did I do that? It wasn't magic at all; it was a bit of mathematics. Actually the message sent by the computer isn't the whole thing, but just the top four-by-four block. This is actually the message they want to send, I'm going to separate this off. The message sent by the computer is actually this top block here and the other digits are used to keep check of what's happening inside the message. And actually the bottom here, if you look at the bottom column, this number here will be a one, if there an odd number of ones in this column, OK. And if there's an even number of ones, so in this column I've put a zero, OK. So when you turned one of the things over, it didn't check out. So, for example, if I turn that over then I've got, well they're meant to be an even number of ones there, so I know there's a mistake in that column. And the same thing for the rows over here. Why I'm telling this to you is because you're going to have a go yourself now, to see if you can correct a mistake. You can work out which column is wrong, by checking something's wrong down here. And which of the rows is wrong. Do you want to take on the challenge?

Lauren

OK.

Marcus

Alright, OK. We're going to blindfold her, and you can close your eyes as well, if you want to do a challenge, so let's get you over there. I won't be so vicious as Andy, he almost took my head off there. OK, we're also not going to show the viewers at home, so they can have a challenge at this as well. I'm going to change one of the numbers over now. Yes, cover your eyes and we'll see whether you can correct the error. OK, I'm done. So let's see whether you can do it. Zero's even, well done, something in this column then is wrong, yes. What about the rows?

That's right, even number of ones there. So it's the first row, no you had the second column, that's right. So it was this one, exactly right. So give her a big round of applause for correcting the error, well done.

Now you might like to have a think about what happens if one of these numbers gets changed on the rows and the columns which are doing the checking. You can even correct those as well. Error correcting codes like this are used all over the place: in CDs and satellite communication. For example, when NASA sends pictures back from outer space, there's a lot of interference. They use even more sophisticated mathematics, this can correct one number, but they need to correct lots of numbers. For example, here's a picture, it was sent back before it was corrected; this is Saturn – pretty fuzzy. But using the mathematics error correction they managed to change it into this. Much more crystal clear. OK, we're going to take a break in a moment, and here's a code for you to try and crack whilst we're away. So far all the codes we've been using have been trying to aid communication, but in the rest of the lecture we're going to look at some codes that have been used to keep things secret. And I'll show you how mathematics can be used to make and break these secret codes, so come back after the break to find out how mathematics can be used to crack this secret message.

Part 2

Marcus

Welcome, welcome back to The Number Mysteries and the case of the uncrackable code. Throughout history codes have been used by governments and spies to carry information through enemy territory. And in most wars there's been a battle between the code makers and the code breakers. In the rest of the lecture I'm going to reveal some of these secrets.

Now this message you've been looking at during the break, looks like a complete loads of gibberish, but it's actually been encoded using something called the Substitution Cipher. This is a very famous cipher used throughout history by people like Julius Caesar, and Mary Queen of Scots also used this cipher. The way it works, is that each letter is translated into another letter, so for example, instead of writing an A you might choose to write a P, so A is always changed to a P. C, for example, always changes into a T. Now as long as the sender and receiver have agreed how to scramble the letters around, they can decode each other's messages. But to everyone else, this looks like a complete load of gibberish. In fact, how many different codes can you make like this? Well 26

letters, the different ways you can scramble around: it's an amazing 400 million, billion, billion different ways that you can scramble this. So now we're going to try and find which one of those 400 million, billion, billion I've used to encode this message.

Now, so you might think this looks really secure, I mean how on earth do you crack this? Well, unfortunately, the Substitution Cipher has a really big flaw: its security crumbles in the face of a statistical technique called Frequency Analysis. Now in the ninth century an Arab mathematician named Al-Kindi wrote down the first way to try and crack these codes. And it works on a very simple principle, the fact that some letters in languages occur much more often than other letters. So, for example, in the English language, what is the most common letter that's used? Do you know? What do you think it is? E, that's right, E is the most common letter. So here we've got a Frequency Analysis of which are the most common letters and which are the really rare letters. So, in fact, E occurs about 180 times more often than the letter Z for example. So here's E, E is the most popular letter in the English language, and for example J is actually a very rare letter. The second most common letter in the English language is, in fact, T, and so you can see the height of T there, it's pretty high. After that we get vowels, we've got three vowels which are quite popular. We've got A, and then I, and then O, are also quite popular. OK, so if we can use this to actually crack the codes that I gave you during the break. Before you came into the lecture, you were all given this code and one letter, and you were asked to count how many times your letter occurred in this message. So we're going to try and find which is the most frequent letter here. Has anybody got a letter which occurs 10 times inside this message? No, what about 9 times, anyone with 9 times the letter? OK, so what's your letter? W, so it's probably a W is E inside this code. So let's change the W into an E and see if we can see any, sort of, more insight. Let's change the Ws into Es. OK, so that's the first indication. Now we need to find the second most common letter, and hopefully that might be a T, so what about 8 letters, anybody with 8 letters? OK, what's yours? U, U occurs 8 times, so that's probably going to be a T. Let's change all the Us into Ts; that's looking much better. We're getting a little of insight, we've cracked two of the numbers. OK, that's 8, what about 6 and 7, anybody with letters that occur 6 or 7 times. OK, so what's your letter? C, anyone got anything different from a C? OK, what's your letter? B. So C and B are likely to be maybe some of these vowels, OK, let's see; look there, a B is on its own. So it's very likely that B is going to be a vowel. Something like, well A is often a letter which is on its own, or, I as well, maybe I'm doing something, or it's 'a' something or other. So let's try A, let's try the B changing into an A. OK. Well actually we're pretty well in here because look

at that last word there: it's T, something very popular, EE. And I can't think of a vowel that I would put in there, so, now this message is very short and its Frequency Analysis is not an exact science. It gets better and better the longer the message is, so that may not be actually one of the vowels, but can you think of a word, T something EE. Yes, what do you think it is? Tree, OK so we think the C might be an R. So let's change all the Cs into Rs, that's one of the common consonants. We change all the Cs into Rs. We're really into here. OK, it is, A YEAR TREE. OK, but the Y's not quite right. Does anyone think they can crack this message yet? Yes, what do you think it is? A P, you think it's a pear tree? OK, so who thinks they've cracked the whole message? Oh, you're all in there. OK, right, you want to sing it out then: On the first day of Christmas my true love sent to me, a partridge in a pear tree. That's right. Actually, just by cracking four letters, by using this Frequency Analysis, we're in and we managed to crack it. So that's amazing. We found the one code, out of 400 million, billion, billion, just by using this Frequency Analysis. This simple mathematical trick means that no matter how you try and disguise the message, using the Substitution Cipher your secret is probably going to be out.

To prevent codes being broken, a sender needs a way to scramble the letters so that his Frequency Analysis doesn't work. Now this is the famous Enigma machine, it was used by the Germans in the Second World War and it was a vital part of the German war effort. They made actually 30,000 of these things, and they were used to send messages between U-Boats and the front line and things like that. The way it works, it's actually set up at the moment, as a Substitution Cipher. But the person who was sending the messages would first of all look up in a code book to see how these rotors inside here should be set. He would set the rotors and then close the lid, that would set it as a Substitution Cipher, and then he would press the message he wanted to send. So, for example, if he wanted to send a T to start with, press the T and the U would light up, so that's a Substitution Cipher there. But you might have seen that actually one of these rotors clicked on, so that's actually going to scramble the letters in a completely different way now. So if I press T, it won't be the U that lights up, but we've got the K lighting up here. The rotors kicked on again, it's going to scramble the letters in a completely new way now. So press T again, lights up a G. So the Substitution Cipher T would be the same letter each time, but this one, I've got three different letters because each time we get a new scrambling of the letters.

So how does this machine actually work? Well we've got a simplified Enigma machine over here. And I'm going to need two volunteers to try and help explain

how this Enigma machine works. OK, right, I'm going to have this volunteer over here. Now you stay there for a moment, because you're going to actually decrypt the message once we've encoded it on the Enigma machine. So we're going to need to... Ritchie here is going to put some earphones on you, I think you're going to get to listen to some music, and we're going to blindfold you as well, OK? So we're going to leave him over there, and we need somebody to encrypt a message, OK. So, let's have you there, do you want to come out? Great. So we're going to encrypt a message, we mustn't tell him what the message is; I'll tell you in a moment what the message is. Can he hear or see anything? Pump up the music. OK, I think he's well out of it. So now we're going to send the message bee, a bumblebee, OK, B E E. Right, so what I want you to do is take this ball and find the letter B at the top, and that's like typing in a letter on the Enigma machine, so here we go. What we need to do is tuck the ball under there and put it down that shoot. OK? So B is going to be encoded, there we go, off it goes. Where is it coming out? Do you want to go round and see what? So this would be the light, lighting up on the Enigma machine, and what is it? A D? OK, so our first letter, a B has become a D. OK, if we left the machine like this, then it would just encode it like a Substitution Cipher, but the clever thing is that the Enigma machine clicks on one, the rotor clicks on and scrambles the letters now, in a completely different way. OK, if you want to take the ball out, we're going to encode the letter E now, so let's find E at the top. So you're going to press the E on the Enigma machine, and which letter have we got now? C. OK, let's put C so the E has become a C. Now we're going to encode E again, but remember the machine clicks on... the rotors click on, so if you want to take the red ball, we're going to pop it in E again. Now the clever thing is, of course, that hopefully this is going to be a completely different letter, so yes, it's popping out here. OK, so now we've got the letter A. So anybody looking at this would think these are three different letters. Right, OK, so now, we're going to get somebody to decode your message. Well let's give her a big round of applause, at least for encoding our message. So if you go back, OK, we can take our volunteer out of his dreamy world. Yeah, I wonder what he's been listening to, X9Y, maybe? Welcome back. OK, come and decode a message then. What have you been listening to under there? No idea what it was? Some Second World War music, maybe. So I want you to come over here, and what's your name, sir?

Wassim

Wassim.

Marcus

Wassim, OK. So you're going to decode a message. Let's come and have a look at your message, you were sent this by the Enigma operator, DCA. And nobody

knows what it is, OK, so now. Well you don't know what it is, everyone else here knows what it is. So what we need to do is re-set the way the Enigma machine, it's quite clever. You re-set it to how the person encoded the messages, type the secret message in, and out comes the decoded messages. So we're re-setting it, this is slightly different from the Enigma, we need to turn it up side down, but we do, well Evil Andy is even helping, that's great. OK, well the way this machine was set up this morning is with the red lines down here. Now you need to feed in a D to start with, so we need to find D at the top, this is like typing in the message; this is the encoded message. That's right, so if you put your ball, if you slip it under there, it'll go down. OK. Oh it's coming out the back here. Right, so what's the letter that lights up? A B? OK, so the D became a B, and then the machine clicks on, wait a minute, that's right, you have to wait for the Enigma machine to click on, remember it's this rotor that is turning. So now we feed in the letter C, that's coming out as an E, OK. And now we click on again, and we've got to put in the letter A, right. Ended up as an E again. So you probably wouldn't have expected that because you've got CA and that one comes out as an E. So it sounds like your operator is trying to tell you that a swarm of bees are about to come in, so we'd better chase you back to your seat. Give him a big round of applause for decoding our Enigma machine.

Now this is how the Enigma machine worked. It's an extremely good method of encryption, but it isn't completely foolproof. Polish and British mathematicians during the war, managed to crack the Enigma code by finding that there were certain patterns and structure in the messages that they were detecting. Thanks to the mathematicians at Bletchley Park who cracked this code, it's said the war was shortened by at least two years. Now the mathematicians that broke the codes at Bletchley Park actually went on to create the new generation of codes. And I'm going to reveal how they work, after the break, but before we go, here's a little bit of a challenge for you. Now you might remember my favourite numbers are prime numbers. But this number here, 126,619 is not a prime number. It's in fact two smaller numbers multiplied together, two primes. Now, during the break what I want you to do is to try and find the two primes which multiply together, give this number 126,619. And I'll show you, if you can do that, after the break, why you've cracked a code.

Part 3

Marcus

Now before the break I set you a little challenge, could you find the two prime numbers, which multiplied together, give the number 126, 619? Now anyone's

who's actually managed to do that has actually cracked a code. And it's the code that's being used to protect messages on the internet. Before I reveal the two numbers, I want to do a little demonstration to show you the power of this mathematic code. I'm going to need two volunteers, but they're very special volunteers, because in this demonstration, whenever somebody sends a message in the cryptographic world, it's always Alice sending messages to Bob. So I wonder do I have anyone called Alice in the lecture theatre? Ha ha, very good. OK, you'd like to be Alice, up comes Alice, a big round of applause to Alice. Excellent. Now Alice here, if you'd like to stand here, welcome Alice. Now Alice is going to send a message to Bob. So do I have a Robert or a Bob in the? OK, here's Bob over here. Right, if Bob would like to come up. So Bob's going to stand here, now Bob actually lives in Australia and he runs a bookshop. And it's a bookshop online, so he's got a website. And Alice here, over in London, who's never met Bob in Australia, has gone on the website and found a book that she wants to buy. So she wants to send her credit card immediately and buy this book. Here's your credit card. OK. But Bob, you published on your website a code number and that's this number, 126,619. Actually, this key, it's like this code number, which you can pick up from the website, and its code number is basically what this key is. So this is the number, 126,619. And with this key, you can now lock your message away, and make it encrypted. So that's what we're going to do with this box. This is going to represent the encryption, so let's open the box up. Alice, if you'd like to pop your credit card, just pop it in there. That's the credit card number being put away and now you're going to encode the credit card number with this number 126,619. Let's put this in, turn it around, and we should see it go from unlocked, to locked, excellent. OK, now this credit card has been locked away. What's actually happened is your computer has done a computation, with your credit card number and this number, 126,619, and it's scrambled the number together. That's sent across the internet, all the way over to Bob here in Australia. But hold on, I can also get a copy of this key, and all the previous codes we've seen, provided I know how to encode a message I can also decode it. So I'm a hacker, I want to get your credit card number. Surely I can use the key to unlock the box? But this mathematical code is very special and it's not the same key which unlocks the box. If I try and get in, hack in to your credit card, I just can't seem to unlock the box. It stays locked. And this is something very special. The Enigma machine, once you know how to encode a message, you can decode it. What's special is that Bob over here in Australia, he has two secret keys, which are actually made out of this number. But here's the secret, the key which will unlock this is actually two keys and the two keys are made out of the numbers P and Q which give this number. So the numbers which you need are the two prime numbers, and these are numbers

you're trying to find during the break. 127 and 997 are the two numbers which will help us to unscramble this computation. So there. If you want to put one key inside here, right pop it in that side, and I'll put this one. And we'll put it in, hopefully, and turn the thing. The thing will go from locked to unlocked. So it's these two prime numbers that you need to unscramble the computation. Hopefully this is now open, great, and here's the credit card number. So you've managed to get the credit card number, out of the box. OK, so that's how you send a message. There's one number to encode messages, but to undo the message you need to know these two prime numbers. Well let's give Alice and Bob a big round of applause for sending a message across the internet.

Hold on here, I'm a hacker, OK, so the key, this key didn't open the thing, but I know that if I look up on Bob's website this number, and I can find the prize P and Q that you were looking for during the break. Well, if I know those, I know how to decode a message. So I just need to split this public number into these two primes, and I'm into Bob's website. Now this is a very small number, so it's quite easy to find these primes, P and Q: 127 and 997. But real websites use much larger numbers than this; and it's almost impossible to find the two primes which built this number. So, for example, the mathematicians who invented this code are so confident in its security, that they're offering \$200,000 to anybody who can crack this number here. It's a 617-digit number, 617 digits, but it's two prime numbers multiplied together. They know what the primes are, they multiply them together and they publish it on their website. Now you might think a super computer could probably crack this code, maybe if you set it. But a simple computer would have to check more primes than there are atoms in the universe to be able to find the primes which divide that. So it's almost impossible to crack this number.

So, to make a code what you need is to find two prime numbers. That's very easy. And if you remember, prime numbers, they're rather like atoms in the chemistry. We've got some atoms over here, which Evil Andy is bringing on. Boo! So Evil Andy is going to, just the same way, we've got two prime numbers, two atoms, multiply the two prime numbers together to make a code – it's a little bit like mixing two chemicals together. If you're ready Andy: three, two, one. OK, so you multiply the two numbers together, that's very easy. But to try and undo this chemical reaction that the Evil Andy has done is very difficult, and that's the same with a code. Finding the two primes, multiplying them together is really easy, but to try and separate them and take the two primes, that's really difficult. So prime numbers are literally, the whole, they're behind the whole of internet security. Without

primes and mathematics, you wouldn't have Amazon.com or eBay and the world would be a very different place. But even if these prime number codes get cracked, there are even more sophisticated codes already being implemented. In fact, every time you fly, the flight paths are being protected by a new code called Elliptic Curve Cryptography and the million dollar prize is for understanding the mathematics behind these elliptic curves. Now maybe if you managed to crack this problem, the million dollars you won't worry about, because you may become the most powerful hacker in the world. (PHONE RINGING.) Let's hope that's Bletchley Park, let's go and see. OK Tony, Tony are you there now?

Tony Yes, I am, yes.

Marcus Great and have you managed to decrypt our message? I see your Enigma machine there.

Tony Yes.

Marcus You are... you think you've got the numbers?

Tony We've been working hard on that. We think we've got them, Would you like me to give them to you.

Marcus No, please wait a minute, I'm going to get a volunteer to try and open our safe for us, OK? Wait until we've got a volunteer and then I'll get the numbers off you. So, would you like to come up? OK, come up. Right, let's go over to our safe. Hopefully we can get all these chocolates now, if they've managed to crack the code. So what's your name sir?

Dan I'm Dan.

Marcus Dan. We're going to get the number from Tony up in Bletchley Park. So, Tony if you could give us the first number please?

Tony 2-7. 27.

Marcus OK, so you need to turn the dial to 27, see the zero mark up there, so turn it this way. OK? Right, 27, yes we've got the first one. Second number please Tony?

Tony 1-8. 18.

Marcus OK, so you need to turn the dial to 18. That's great. And the third number?

Tony 2-8. 28.

Marcus OK, so moving on to 28. Any more numbers Tony?

Tony That's it.

Marcus So let's see whether we can open the safe. Yes it's turning. OK, there should be some chocolate inside here. Hmm, there are no chocolates. Andy? Somebody get Andy. Well, Tony thank you very much for cracking our code, but somebody's made off with all our chocolates. That's outrageous. Well we can give poor old Dan here a few wrappers to take away. I'm really sorry about that, but you have had the satisfaction of breaking one of the most sophisticated codes in history. So let's give Dan a big round of applause.

I don't know, that Evil Andy. Now the information age is built on mathematical foundations, every time you do business on the internet, or watch a DVD or switch on your television set, just remember that's all thanks to a mathematician somewhere who's come up with a clever way to code the world around us.

Man Got him.

Marcus Right, bring him in. Here's the Evil Andy, boo! I don't know, swag bag here. OK, your punishment is to help me to share all of these chocolates with our audience. Good night, till next time.

Andy It's a fair cop.

© Royal Institution and Five 2007