"Decoding Nazi Secrets"

PBS Airdate: November 9, 1999

Go to the companion Web site

During the following program, look for NOVA's Web markers which lead you to more information at our Web site.

NARRATOR: In spring 1946, an order came through to destroy all the records of what had been the Allies' most secret operation of World War II: the codebreaking unit at Bletchley Park.

UNIDENTIFIED WOMAN: Everything was destroyed, there wasn't a scrap left.

NARRATOR: By mid 1940, the German Army had conquered all of western Europe. Hitler was tightening the noose around Britain. In the Atlantic, German U-boats were decimating Allied convoys, threatening to cut off Britain's only lifeline. But Churchill had a secret weapon, the strangest military establishment in the world. Crossword fanatics, chess champions, mathematicians, students and professors, Americans and British, all came here with one common aim: to unlock the secrets of the Enigma, a machine that concealed Germany's war plans in seemingly unbreakable code. If Enigma could be penetrated, everything Hitler plotted would be known in advance. At Bletchley Park there unfolded one of the most astonishing exploits of the Second World War. Many here had never seen a code before, yet it was their job to find a way to crack Enigma. In the process, they devised ingenious codebreaking machines that were forerunners of the modern computer. But everything they did remained classified for 30 years. Tonight NOVA reveals the secrets of the men and women who helped turned the tide of victory and shape the future.

NARRATOR: In 1939, Germany introduces a devastating new kind of warfare, blitzkrieg. Lightning attacks by tanks and planes bring Europe to its knees. Blitzkrieg depends on surprise, demanding speedy communication. So radio is crucial to the attack plans. Every day the skies are full of German radio signals. The German high command has trained thousands of wireless operators in preparation for the conquest of Europe. Their job is to be able to interpret Morse code in any conditions. But there is still the problem of how to keep the messages secret. So the German military has adopted a seemingly invincible code-making machine. The Enigma turns a message into unintelligible gibberish, letter by letter. When the message is sent in Morse code, all an enemy would see is a meaningless string of letters. But when the German operator at the receiving end types the coded letters back into his Enigma machine, the real message appears. In this way vital war plans remain totally secret. The high command never wavers from its belief in the security of Enigma. They are so confident that they deploy the Enigma throughout the German war machine. They never imagine what was about to happen at Bletchley Park.

NARRATOR: This is the machine the German high command believed would protect their secrets. This is the Enigma.

TONY SALE: Its complexity's enormous. I mean, if I sent just one message on an Enigma machine today it would still take a super Cray computer, the fastest in the world, a year to go through searching for that one message without supporting evidence as to what that message might have been.

NARRATOR: Long before the war began, the airwaves were full of coded messages as Hitler prepared for battle. Cracking the German ciphers became the priority of a special British Intelligence unit. In 1938, the unit, known as the Government Code and Cipher School, or GC&CS, moved into Bletchley Park, an ornate mansion 50 miles north of London. From this rooftop room, wireless operators contacted listening stations all over Britain that were intercepting German messages. Bletchley Park's code name was Station X. The challenge of breaking the Enigma demanded a special kind of talent. GC&CS set about recruiting.

ANDREW HODGES: The people who a few years earlier were regarded as too young and not knowing anything of importance, of not being real people, not having, not being significant grown-up people, suddenly they were the people who held the keys to the Reich.

ARTHUR J. LEVENSON: Codebreaking was a somewhat esoteric profession. But it wasn't clear exactly who would make a good codebreaker. People who were recruited were asked whether they did crossword

puzzles. And if they said they did and enjoyed doing them, and did them well, that was generally enough to get you in. We discovered people of a whole variety of backgrounds did very well. Anthropologists, Egyptologists, paleontologists, and even an occasional lawyer turned out to have the knack.
NARRATOR: Bletchley Park evolved into a unique operation in which military discipline, uniforms, and rank no longer mattered. The sole imperative was to break the Enigma, and break it as quickly as possible.
DONALD MICHIE: At that age you can just take fire and blaze away, half out of your mind with enthusiasm and dedication, you're not married, you don't have to worry about the kids and the rent and so forth. And during that sort of short period of your life you can live like a madman and, you know, take almost no sleep and - determined to do it.
NARRATOR: But youth and determination weren't enough. Mathematicians were enlisted to take on the daunting complexity of the Enigma. Only a completely new approach to codebreaking could help to penetrate its secrets. But if the work at Bletchley Park were to succeed, absolute secrecy was essential. Some of the recruits had no idea of the purpose of their work.
GWEN WATKINS: Most of us who were among the - what shall I say, the hoi polloi, the lower grades, never knew what went on at Bletchley Park. The only time I realized what we were actually doing was when I was shown a code book which had just been captured and rushed to Bletchley from a captured plane, and of course we had no plastic envelopes or anything then, the poor thing was just given to me as it was and I was horrified to see a huge bloodstain on it, the blood 'round the edges was drying, but the blood in the middle was still wet and I realized then that somewhere was this German - this German air crew bleeding, still bleeding while I was decoding - I was writing out in modern German their new code book, and that did bring the war very close.
NARRATOR: The Germans were supremely confident in the Enigma. Its basic principle was simple, but it could scramble messages in millions of different ways. Pressing one typewriter key would light up a totally different letter. An electrical current was sent from the keys to the letters through a series of rotors. Each time a key was pressed a rotor would turn, altering the wiring and so changing the letter that was produced.
TONY SALE: The total number of ways in which the Enigma machine can be configured for any particular message is 150 million million million. So it was an enormous complexity which was why the Germans thought it was completely safe.
NARRATOR: The Enigma was first developed as a commercial encryption device in the 1920s and patented in London. German banks and railways were among its first customers, but the German military was quick to see its potential. Each day German operators in the field received a new set of instructions from base on how to set up the Enigma. They had to make three adjustments so that both the sender's and receiver's machines would match. First, which rotors to put into the machine and in what order.
TONY SALE: The rotors contained one of the central secrets of the Enigma machine, which was the cross wiring inside the wheels. The whole of this maze of wiring inside changed every time a letter was entered and that's what gave the Enigma machine its vast complexity.
NARRATOR: The second step was to change the wiring of each rotor by adjusting the ring of letters around the rim - 26 combinations on each wheel. The third step was the plugboard. Using his secret instructions for the day, the operator could wire up each typewriter key to a totally different letter.
TONY SALE: This was what the Germans thought was the killer cryptographically. This plugboard enabled you to transpose letters completely, a pair of letters. Now because there are 26 sockets on the front of the Enigma machine, you can plug these pairs of letters together in an absolutely astronomical number of combinations, about one-and-a-half million million combinations that you can use on the front.
NARRATOR: Once the machine was set up, the message was encoded letter by letter. These letters were then sent by Morse code to the receiver at the other end. The Germans were never shaken in their belief in Enigma's invincibility. At first, all the codebreakers had were meaningless groups of coded letters and endless patience. And in the first months of the war the new recruits were getting nowhere.
TONY SALE: At the beginning of the war there was a great difficulty because although we had intercepts which we knew were enciphered using the Enigma machine, we didn't know enough detail about the machine to be able to even begin to find any method of breaking it. Unless you've got the exact key you just cannot get anywhere with it at all and this is a major difference from any code systems prior to that, that the Enigma machine, there's no sense of nearness, you're not nearly at a solution. You've either got the solution or you haven't got the solution.
NARRATOR: The search for a solution began long before the war. Starting in 1931 and continuing for seven years, a hard-up German army clerk secretly obtained more than 300 documents, including the instructions and settings for the Enigma machines. He sold them to the French Secret Service, but their

cryptographers showed little interest. Next the stolen documents were offered to the British Secret Service. At this stage, GC&CS was skeptical that Enigma could be broken and politely declined the offer. Finally the documents went to the Poles. With Germany breathing down their necks, their response was very different. A deal was struck. With the stolen documents in hand, three brilliant young Polish mathematicians, Zygalski, Rozycki and Rejewski, set to work on the Enigma. The Poles soon realized that they had to figure out how the Germans had wired the Enigma's keyboard to the first rotor. Since any typewriter key could be wired to any letter on the rotor, the number of possible wiring orders was astronomical. But if the Poles could work this out, it would be a vital first step in breaking the Enigma.
TONY SALE: Rejewski had a flash of inspiration and he thought, what about if they've been stupid enough to just use ABCD as the order round the rotor, and they had, all the multitude of millions and millions of ways in which they could have scrambled the connection from the keyboard to the entry point, and they'd just chosen ABCD. And Marian Rejewski in desperation tried that, it worked, and suddenly he'd got the internal connections of the whole of the German forces machine.
NARRATOR: But in 1939, on the eve of the invasion of Poland, the Germans added an extra choice of rotors to the Enigma and the Poles could no longer read any of the messages. In desperation, they invited British and French officials to a secret meeting in a forest near Warsaw. They revealed how they had previously broken the Enigma. The British were astonished.
TONY SALE: And Dilly Knox, he was one of the members of the team that went there, and the first thing he asked Rejewski was, what is this mapping from the keyboard to the entry rotor, and Rejewski said, ABCD. And Dilly Knox went, oh God, we never thought of that, it's too obvious, why didn't we think of that?
NARRATOR: Within weeks of that meeting, Poland was invaded and war broke out. The Polish cryptographers had given Bletchley Park their own replica of the Enigma machine, but the extra rotors the Germans had added meant that the codebreakers were still in the dark. As the flow of German messages increased, at last they began to see a way of achieving the impossible. The starting point was the messages themselves. The British had set up a worldwide network of radio listening posts operated by the military, the post office, and even the London police. They were known as Y Stations.
JOAN NICHOLLS: Wherever the Germans were, we were listening. When there was a lot of excitement, the wires would be absolutely humming with Morse, they'd be transmitting all over the place. We'd really have cramp in our fingers sometimes, trying to write it down non-stop.
NARRATOR: Round the clock and around the world, thousands of operators were writing down meaningless groups of coded letters, the raw material for Bletchley Park. Their approach to cracking the Enigma began with another Polish breakthrough. One of the special procedures the Germans followed in setting up their machines was known as a double indicator. It was to be the Enigma's Achilles' heel. The instruction sheets for each day told the German operator how to set up his Enigma. They specified the order of the rotors and the position of the ring of letters around each rotor. The sheets then provided instructions for wiring up the plugboard. All Enigmas on a network had to be set up identically for the system to work. But there was one extra level of security. If the enemy captured the instruction sheets, they would be able read all the messages. To prevent this, each message had its own secret rotor setting, chosen by the operator. First the operator had to pick three random letters. He sent these in plain text to the operator at the receiving end, allowing that other person to line up his machine identically.
TONY SALE: But now the operator had to be able to tell the operator at the receiving end what the actual message settings from which he was going to start enciphering the message, and that had to be conveyed to the operator the other end but not revealed to any interceptor, and the way that they chose to do this was to use the Enigma machine itself to conceal this message setting.
NARRATOR: So the operator encoded a second group of three letters as the secret message setting itself.
TONY SALE: And supposing he thought of SWJ, and when he keys in SWJ the lamps light up ITV. Because the Germans felt that radio transmissions might be unreliable they went a step further and they actually asked the operator at the sending end to key in the message setting twice. So the procedure was to key in SWJ SWJ and to note down all six lamps that lit and that was a crucial mistake because the repetition of the message setting gives a cryptographer a toe-hold into finding out what it actually is, repetitions are always bad news in cryptography.
NARRATOR: By encoding the same letters twice, the Germans gave the codebreakers their first clue about the setting of the Enigma rotors. Soon there was a second clue. The Poles had noticed a strange quirk in the way the rotors worked. In about one out of eight intercepts, the Enigma was turning one of the letters in the message setting into the same coded letter twice. The mistake of sending the message setting twice was

revealing a flaw in the machine itself. Although it was designed to produce random coded letters, there were certain situations in which the Enigma was much less random than the Germans believed.
DONALD MICHIE: There is no such thing as a random, a truly random sequence that can be generated by a purely deterministic machine. That just cannot be. It's part of the definition of randomness that it cannot be explained or predicted in any way whatsoever.
The whole game of cipher design is to design machines which are flawed, they have to be, but in which the flaws are as small, inconspicuous as possible.
NARRATOR: It was just such a flaw that broke the Enigma. Bletchley Park called the repeated letters "females." Only a few configurations of the machine could produce these females. If the codebreakers now worked their way through them, they would find that day's settings. The codebreakers produced huge cards, known as Jeffries sheets, with holes punched through in an alphabetical grid representing the wheel positions that could produce females. By lining these sheets over each other, the codebreakers could hunt through the wheel positions to find out how the Enigma had been set up for that day.
PAM BREWSTER: They were, John Jeffries, they were really his rather special baby. And they were on sort of cartridge weight paper. Not very thick card, they got very dog-eared. And as far as I remember there were two alphabets that way and that way. It was like solving a very difficult crossword puzzle. You could actually see it happening. And the triumph when you found it worked, that was fascinating.
LEVER: Marvelous. Absolutely marvelous. There's nothing like seeing a code broken. That is really absolutely the tops.
LESLIE YOXALL: The one thing that was very interesting was that people were very reluctant to go home at the end of the shift. There was a certain amount of "Move over!" You know "Let me sit down and get on with it." People wanted to hang in there.
ALAN ROGERS: On one occasion I was on the evening shift but when midnight came I was stuck in a message that was, had gripped me so hard I worked right through 'til breakfast time. From four o'clock in the afternoon to breakfast the next day. Simply because this had to get done.
NARRATOR: In the spring of 1941, the naval war was building up in the Mediterranean. Hitler had joined forces with the Italian Fascist Mussolini. Both dictators were dreaming of global empires. The Allies knew that the Germans had given Enigma machines to the Italians. One of the codebreakers trying to break in to the Italian messages was 19-year-old Mavis Lever.
MAVIS LEVER: Sometimes you'd have to spend the whole night assuming every position that there could be on the three different wheels, and there we called them Red, Blue and Green, the wheels, I think they did too. So that you would have to work at it very, very hard and it was that I think that made one pink-eyed and after you'd done it for a few hours you wondered whether you'd ever see anything when it was before your eyes because you were so snarled up in it all.
NARRATOR: Mavis and the other codebreakers didn't know it, but they were about to make their first major impact on the war.
MAVIS LEVER: The one that came up was real good stuff, drama, "Today's the day minus three," just that and nothing else. And so of course we knew that something was going to happen, the Italians were going to do something, the Italian Navy, in three days' time. Why they had to say that I can't imagine, it seems rather daft but still they did.
NARRATOR: The British fleet was based in the Egyptian port of Alexandria under the command of Admiral Andrew Cunningham. Bletchley Park intercepted a message that would lead the Admiral to hatch a clever plan.
MAVIS LEVER: Well then a very, very large message came in which was the battle orders, how many cruisers there were and how many submarines were to be there and where they were to be at such and such a time, absolutely incredible that they should really spell it all out.
NARRATOR: Mavis had decoded just the message that Cunningham needed to outwit the Italians.
MAVIS LEVER: It was 11 o'clock at night and it was pouring with rain when I rushed, ran, absolutely tore down to take it to the Italian - to intelligence to get it across to Cunningham.
NARRATOR: Within hours the decoded message was on its way to Cunningham in Egypt. The Italian fleet was gathering off Cape Matapan on the Greek coast. Their plan was to attack a British convoy at midnight. Alexandria was a nest of spies. The problem for Cunningham was how to act on the message without giving his plans away. If he led the fleet out to sea the Italians would know immediately. Cunningham embarked on an elaborate ruse to fool the spies. He wanted his enemies to believe that all was quiet.
MAVIS LEVER: He did a real Drake on them, well more than Drake, because he played golf and pretended he was, you know, just going to have a, you know, a weekend off.

SIR ROBERT ATKINSON: Admiral Cunningham was a crafty fellow, and by subterfuge he was able to lead the enemy to think he was socially engaged doing something else, and I've no doubt when he went ashore at Alexandria to play golf, that information was in Italy within about five minutes.
NARRATOR: But at night Cunningham slipped back on board and led the British fleet out to sea, to the precise spot where the Italian ships were gathered. The ruse worked. Cunningham caught the Italians completely off guard. That night the Italians lost nearly 3000 men, the cream of their navy. It was the first major coup for Bletchley Park.
NEWSREEL: The Navy does it again. Here is the British Mediterranean fleet preparing for what proved to be the greatest naval engagement so far fought in this war. The Battle of Matapan is one more proof that Britain is the unchallenged ruler of the Mediterranean waves.
NARRATOR: The Navy were the heroes of the Battle of Matapan. Bletchley Park was of course never mentioned, but the codebreakers had their own reward.
MAVIS LEVER: Then Cunningham himself came, it was the first thing he wanted to do when he came was to see the actual message that had been broken, and he was very nice and we had a drink, and we were in this little cottage and the walls had just been whitewashed, now this will show you how sort of silly and young and giggly we were, but we thought it would be jolly nice if we could get, talk to Admiral Cunningham and get him to lean against the wet whitewash and go away with a white stern. So that's what we did so, you know, it's rather terrible, isn't it, that on the one hand everything's so - seems to be so very organized, and these silly young things are wanting to snare the Admiral.
NARRATOR: But their joy was to be short-lived.
TONY SALE: And then disaster struck. The Germans issued a decree, no more double enciphering of the message setting, just single enciphering. Catastrophe, suddenly the Jeffries sheets didn't work and so suddenly darkness fell.
NARRATOR: Gloom descended not only on Bletchley Park but on all British cities. For months, relentless bombing had become part of everyday life. The Blitz was a war of blood and nerves.
SARAH BARING: Well, there was one very good remark is, the only good German is a dead one. We felt very, very strongly. Well, they'd bombed us, they'd - every day, every night - with Heinkels and Dorniers. They'd killed a lot of people in London and in the cities, you couldn't have any pity for Germans under those circumstances.
WINSTON CHURCHILL [voice over]: What a triumph the life of these battered cities is over the worst that fire and bomb can do.
NARRATOR: During the grim months of the Blitz, Bletchley Park was one of Churchill's few glimmers of hope. Access to the enemy's innermost secrets could make the difference between victory and defeat. The codebreakers were working around the clock to break the Enigma. They had divided into huts to attack different parts of the German war machine. Hut 6 was now concentrating on the Air Force Enigma.
NARRATOR: The Luftwaffe's code, nicknamed RED, soon proved vulnerable. Ironically, the German Air Force thought itself so technologically advanced that it was careless about security. For months, Bletchley Park had tried to crack the secret messages from German airfields to their headquarters in Berlin. They had to find a way - and quickly. Hitler was preparing to invade Britain.
JOHN HERIVEL: It was like looking for something in a dark room, one didn't really know what one was looking for, and I thought and I thought. But I had great confidence, I felt, I am going to find some way to break back into the RED.
NARRATOR: John Herivel turned his thoughts to the Enigma operator. There were set procedures to be carried out to prepare each Enigma for that day's messages. The settings of the rotors and the Ringstellung - the alphabet ring around the rotors - were crucial. If the secret instructions were not followed exactly, the security of the whole system would be at risk. But John Herivel discovered that the operators were making a fatal mistake. It became known as the Herivel tip.
TONY SALE: What the operator should do, of course, is when they've done a setting on a cipher machine, you should always spin the wheels so that it randomizes the position. But the whole of the Herivel tip depended on the German operator either being under pressure or lazy and not doing that.
NARRATOR: The operator had to send the three random letters by Morse to the person at the other end so that both machines would be set to the same start position. But Herivel realized that if the operator failed to spin his rotors as he should, then the three letters he was sending over the airwaves - uncoded - would be the secret ring setting. Instructions were quickly sent out to the Y Stations to pay particular attention to the first messages they intercepted each day. That's when the mistake would show up. Hut 6 studied the opening letter groups of the intercepts as fast as they arrived to see if the Herivel tip would work.

Sometimes the operator made only a half-hearted attempt to spin the rotors. So LWZ would become LYB - just a click or two away - or perhaps LUX. But as the codebreakers plotted out each letter group, they would begin to see clusters of letters that revealed the original secret setting. Herivel's tip was working. At last, they had a way to break Luftwaffe RED. The codebreakers could now give the RAF vital information about how the Luftwaffe was organized and what it was planning - even if they didn't always know the details.

PETER CALVOCORESSI: You don't get a message saying, we are going to do the following great things in the next six months of the year, signed Hitler. Nothing like that at all, you don't get anything on a plate. There was a case of an intercept which consisted entirely of figures, random figures, and someone says, I wonder if they are coordinates on a map, and they all turned out to be airfields. You did in fact get from that that they were readying and building up airfields, because they were going to concentrate their forces on attacking Britain. Hut 6 broke the Air Force Enigma every day until the end of the war. And they kept discovering new types of careless mistakes by the German operators that gave them away. To avoid interception, the Germans had to disguise each message setting. They thought they had found the perfect solution: use the Enigma itself to conceal the setting. The operator had already been told to think up three random letters for the initial rotor setting. Now he was told to think up three more, and type them into the Enigma. They would be the key for that particular message, and since they were being encoded, they could be transmitted in complete safety.

ARTHUR J. LEVENSON: On the surface it looks like a foolproof indicator system, the true setting of the message is hidden. However, the weakness was leaving the selection of the three letters to the operator at random, and human beings simply are not random.

NARRATOR: Hut 6 soon saw connections between the two sets of supposedly random letters. Once they got the first three letters which were sent in plain text, they could often guess the second three, which were in code. One operator called Walter became legendary at Bletchley Park. Every day he would set his rotors to the first three letters of his name and then type in the first three letters of his girlfriend's name, Klara.

LEVENSON: One wonderful one: the outside indicator was TOM, and we thought oh, tom-tom, and we thought that, that didn't work. It was TOM MIX, the American cowboy actor from the 1920s, I don't know, I didn't know in Germany anybody knew who Tom Mix was, but apparently he had a following in Germany.

NARRATOR: HIT was almost invariably followed by LER. Even Hitler was helping to break the Enigma.

TONY SALE: They were given the manuals, they were told exactly what to do and how to use the machine, but part of the problem was this myth that the Enigma machine was completely unbreakable. And this was buried deep in the German psyche, so therefore they thought why bother, you know, nobody can break these messages if we use these keys because they're easy.

ARTHUR J. LEVENSON: If you saw LON as the first three, it was almost certain that DON was the second. MAD was RID, BER was LIN.

MAVIS LEVER: In the heat of battle you'd put up dirty words, and I am the world expert on dirty German words. The worst message I ever had come near me was one from the German high command to someone in Abwehr, the German Intelligence, reprimanding them for using these words because, did they not know that young girls were having to decode them? And of course a young girl at Bletchley was devastated because they were - however, they went on doing it, I might say, never mind the reprimand, but it was nice to think the Germans had that side of them that they would think that perhaps they oughtn't to use dirty words in their encodements.

NARRATOR: Despite its success in breaking the Luftwaffe RED code, Bletchley Park had got nowhere with the Enigma of the German Navy - and it was the Navy that was now the problem. By the spring of 1941, German U-boats were wreaking havoc in the Battle of the Atlantic. Every merchant ship sunk deprived Britain of the supplies it needed to survive. Slow-moving convoys of merchant ships regularly crossed the Atlantic to and from America. The United States had not yet entered the war but the convoys supplied half of Britain's food and all of its oil. Although protected by escorts, its convoys were still easy targets for the German U-boats. Hitler had ordered Admiral Karl Donitz to destroy Britain's lifeline.

SIR ROBERT ATKINSON: It was Donitz who realized quite early on that he could defeat the Allies by bringing England to its knees by starving us, if he could break that North Atlantic route then there could be no food, fuel, troops, munitions come to this country and he could win that war by U-boats, and he nearly succeeded.

H.J. KRUG: Donitz tried to build up a kind of elite spirit and everybody was proud to take part in that and we were very eager to join that force, and of course we had been brought up to adore taking risks in the National Socialist period when we were boys. So we were not really aware of the risk.
NARRATOR: Donitz built giant fortified U-boat pens on the French coast. From here his U-boats could strike out into the Atlantic. To attack the convoys, Donitz organized his U-boats into hunting groups or wolf packs, operating along specific patrol lines. As the slow moving convoys crossed the Atlantic, wolf packs of 30 or more U-boats would lie in wait.
SIR ROBERT ATKINSON: Almost every convoy there would be losses. They were very crafty, these German U-boat commanders. They would anticipate our route and submerge in daylight just ahead of the convoy and let the convoy pass over them and torpedo right, left and center and we wouldn't know where the attack had come from.
NARRATOR: Donitz controlled the wolf packs by radio messages encoded in the naval Enigma. Breaking it was to be the biggest challenge faced by Bletchley Park. If they failed, the Battle of the Atlantic - and the war - could be lost. One mind held the key to breaking the Enigma, and it belonged to Alan Turing.
PETER HILTON: Alan Turing was unique, I mean he was a genius, and what you realize when you get to know a genius well is that there's all the difference between a very intelligent person and a genius. With very intelligent people, you talk to them, they come out with an idea, and you say to yourself, if not to them, I could have had that idea. You never had this feeling with Turing at all. He constantly surprised you with the originality of his thinking, it was marvelous.
NARRATOR: Soon after becoming a research fellow at Cambridge at only 22, Alan Turing invented the first basic concept of a computing machine. Bletchley Park suited both his genius and his eccentricity.
ANDREW HODGES: He had funny manners. He didn't like wearing a tie, he always looked untidy, but he quite liked being out in the country where he cycled around, he cycled with a gas mask on during hay fever period. He didn't care what he looked like, he just thought that doing the job was what mattered.
SARAH BARING: He was very shy of women, particularly girls. I don't think he'd ever met any girls before. I did once offer him a cup of tea and he shrank back as if he was going to be shot. And he used to, bless his heart, walk down to the canteen in a curious sideways motion, with his head down. But he was such a star, we all thought he was the best, wonderful thing.
NARRATOR: Alan Turing set himself the challenge of cracking the Enigma. In an attic room at Bletchley Park, Turing began studying the U-boat messages. All he had to go on were the scrambled letters. In an astonishing feat of deduction, Turing discovered exactly how the Germans were hiding the crucial message setting. Unlike the Luftwaffe, the German Navy was leaving nothing to chance. Instead of letting the operator choose three letters at random for his message setting, he had to get them from a list. Although Turing had no information about the naval procedures, he managed to identify exactly how they selected their daily keys from a set of secret tables. Instead of replacing one letter with another, these so-called bigram tables substituted pairs of letters.
UNIDENTIFIED MAN: These codes were printed on rose paper in a ink that would immediately fade out if it got wet, so our orders were, in case of any difficulty, immediately to throw this material overboard or at least soak it in water so it could not be read.
NARRATOR: Brilliant as Turing's deduction was, it was useless without the secret bigram tables, and those were on board the U-boats. Then came an amazing stroke of luck. Captain Fritz Julius Lemp was a hero of the Third Reich. His U-boat, the U-110, had sunk the first ship in the war. In April1941, he set out on what was to be his last mission. David Balme had just turned 20. He was an officer on H.M.S. *Bulldog*, which was escorting a convoy from Liverpool bound for America.
DAVID BALME: We were south of Iceland and we knew we were being shadowed, you'd get the reports back from the admiralty - from the admiralty, you're being shadowed by U-boats. And we always knew we'd be attacked in this area. Suddenly two ships were torpedoed, one after another. It was obvious where the attack come from, and the *Corvette Aubretia* made a very accurate attack on the U-boat, must have got the depth charges at just the right depth.
NARRATOR: Georg Hogel was the Enigma operator on U-110. He had been with Captain Lemp throughout the war.
GEORG HOGEL [voice over translation]: The light went out and we found ourselves sitting in the dark. Only the emergency lights came on. We then tried to restore power and check for water leaks.
DAVID BALME: It was a classic attack, depth charges underneath the U-boat, blew it to the surface. It was the dream of every escort vessel to see a U-boat blown to the surface, because usually they just sink when you do have a successful attack and go down to the bottom.

NARRATOR: This was just the chance that Turing and Bletchley Park had been waiting for. On board the U-110 were the secret bigram tables.
GEORG HOGEL [voice over translation]: Down below we had no idea what was going on above us. But the commander on the bridge kept shouting, "get out, get out!" We asked, "what shall we do with the secret papers?" The order came back to leave everything and simply try to get out. I don't know - but we can't be blamed for following orders. You can't imagine what it was like if you weren't there.
NARRATOR: The Germans abandoned ship, leaving the code books behind. But Georg Hogel had one precious document he had to rescue - a book of love poems to his girlfriend.
GEORG HOGEL [voice over translation]: I went back down and grabbed the key to the place where the books were kept. I got my book out and tried to put it in my pocket. But it didn't fit, it was too big. So I unbuttoned my shirt and shoved it in there. It lay against my chest and that's how I swam for half an hour.
NARRATOR: David Balme led a boarding party across to the stricken submarine. Fearing that the Germans had left men behind to scuttle the boat, Balme went aboard first.
DAVID BALME: One couldn't imagine the Germans would have abandoned this U-boat floating in the Atlantic without someone down below trying to sink her. At any rate I got on, got my revolver out - secondary lighting, a dim blue lighting, was on and I couldn't see anybody, just a nasty hissing noise which I didn't like the sound of. To this day I don't know what it was.
NARRATOR: The rest of the boarding party began to search the U-boat. They had no idea what they were looking for. They did not know about the secret bigram tables. David Balme had never heard of Bletchley Park.
DAVID BALME: I sat down at the captain's desk in his cabin, and suddenly amongst all the things, I think his iron cross was there and I put that into a bag and various odds and ends, but also I came across a sealed envelope, I didn't open it, wouldn't have understood at any rate, being I'm not speaking German, but it obviously was something fairly important, being a sealed envelope in his desk, so I popped it into my pocket.
NARRATOR: Little did David Balme realize that the envelope in his pocket would transform the intelligence battle against the U-boats. It contained procedural handbooks, a U-boat navigational chart, and the vital bigram tables. These documents gave Bletchley Park a major leap forward in decoding. Captain Lemp died in the attack. No one will ever know why he did not scuttle the U-boat or destroy the codes.
GEORG HOGEL [voice over translation]: You can't change things in retrospect. I had to leave because those were the orders. And the unequivocal order was to leave everything behind and go up and climb onto the deck. There was no other way.
NARRATOR: The only document on the U-110 that did not end up in British hands was the book of love poems to Edith. The papers that were captured, including the bigram tables, were priceless. When the documents reached Bletchley Park, the codebreakers rejoiced. The tables and charts would lead to a drastic improvement in fixing U-boat positions, so convoys could be routed evasively around the wolf packs.
VALERIE EMERY: The prize were the bigram tables and they were magnificent, although some of them had got a bit wet and we had to dry them. Geoffrey Tandy, having been at the Natural History Museum, had access to proper drying paper which he brought down by a load, and we had to dry those and clean them up and distribute them as necessary.
NARRATOR: Almost immediately the results were evident. On June 23rd, 1941, Bletchley Park decoded a U-boat message that would save a convoy. It was heading for England laden with supplies, and the codebreakers discovered that a wolf pack of 10 U-boats was lying in wait. Armed with this knowledge, the Admiralty could reroute the convoy and set up a counter attack. The attack lasted five days; two of the U-boats were sunk and the convoy arrived safely. The Allies had a formidable new weapon in the Battle of the Atlantic. But the war was far from over. Frustrated in his attempts to crush Britain, Hitler now dreamed of conquest in the east. In the spring of 1941, decoded Enigma messages hinted at preparations for a massive invasion of Russia. Once the invasion was under way, Bletchley Park began decoding other, more alarming messages.
As the German troops advanced, the SS and police sent signals reporting their mass killings of Soviet Jews. Although no one anticipated the full scale of the genocide, this is now known to be the opening chapter of the Holocaust. When Churchill saw the decodes amidst other evidence, he wanted the whole country to share his outrage.
WINSTON CHURCHILL [archive, radio speech]: Since the Mongol invasions of Europe in the 16th century, there has never been methodical, merciless butchery on such a scale. We are in the presence of a crime without a name.

NARRATOR: Churchill was taking a chance that the Germans would realize their codes had been broken, exposing the work of Bletchley Park. It was a huge gamble. In fact, the head of the order police was suspicious and ordered new restrictions on the sending of reports on the mass killings by radio. Luckily for Bletchley Park, the German high command never lost its faith in the Enigma. But to avoid further risk of exposure, security was tightened and all information resulting from Bletchley Park decodes bore the top secret rating, code word Ultra.
PETER CALVOCORESSI: The Germans didn't attach much importance to intelligence at the beginning. You don't if you're winning. They attached importance to the Blitzkrieg and winning the war quickly. We attached great importance to intelligence because we had our backs to the wall and we had nothing else that we could rely on.
NARRATOR: By the summer of 1941, Bletchley Park was able to crack the naval Enigma in less than two days, due partly to the U-boat documents and partly because they had learned to exploit a crucial weakness of the Enigma machine. When an operator typed a message on the Enigma, the machine would replace every letter with a different one. The letter typed in never came out the same. This was yet another basic flaw in the Enigma that could be exploited. The simple fact that no coded letter could ever be the original letter was vital to the codebreakers in their quest to unravel the messages. As they studied the intercepts, it became clear that the Germans kept repeating certain set phrases. It was soon possible to predict which message contained a particular phrase. Bletchley Park called these phrases "cribs."
PETER HILTON: I remember "Nieder mit die Englander," down with the English. And of course "Heil, Hitler." "Heil, Hitler" was enormously valuable, I mean you should never inculcate in your military, anyway, the tendency to have exactly the same phrase opening every statement of a great victory.
NARRATOR: As military bureaucracy settled into routine, the Germans often sent the same message at the same time every day.
NIGEL FORWARD: There was one remarkable one which we used to, used sometimes to cheer us up as a sort college yell, because it had such a wonderful rhythm. It went as follows: nicht und fliebar, nicht auf Gebaude, gift zu Dusseldorf, puffel swoll," and you can imagine six or seven adults who had nothing better to do on the night shift reciting this and feeling a lot better afterwards, perhaps two or three times in some cases. I mean, that message in itself was pointless. All it said was, "you cannot fly from this place, no building has taken place, signed off, whatever." It would have been much better if they hadn't sent it, from their point of view. It was simply the way into the code.
NARRATOR: When they suspected the presence of a set phrase, the codebreakers then searched for it in a message. Finding the correct position for the crib relied on the flaw in the Enigma. The codebreakers lined their crib up against the coded message. Since they knew the Enigma would never duplicate a letter in the original, if any pairs of letters did match, the phrase must be in the wrong position. They slid the crib along the message until they found a point where none of the letters were the same. This could be where the phrase was located. If successful, they could then work out the Enigma settings for the next 24 hours. The codebreakers became so adept, they would create their own cribs. They would ask the RAF to drop mines in a specific stretch of sea. The Germans would immediately send a message giving a grid reference for the mines. The codebreakers knew the grid reference CF97 would be spelled out in the coded German message. So they used "caesar fritz nein sieben" as the crib to find the Enigma key. Bletchley Park called this gardening. By now the codebreakers were not merely learning about the Enigma, but about the whole system of war communication. Could the new intelligence have an impact on an entire military campaign? The test came in the deserts of North Africa. A new German general was making a name for himself with his aggressive attacks on the British: Erwin Rommel.
MANFRED ROMMEL: My father was what you could call a warrior, he was more a soldier's general, not a paper general. He was very lucky in Africa, not having been wounded, except one day when a British splinter from a shell hit his belt, but the splinter was sticking in the belt and not in his body. Throughout 1941 the desert war swung back and forth across Libya as the Germans tried to capture North Africa. With only radio for communications, Rommel's North African campaign depended on the Enigma.
MANFRED ROMMEL: My father had never an idea that the German code was broken. He could not imagine that something like this could happen.
NARRATOR: But Rommel's strategy had one major weakness. He relied totally on the Italians to bring in supplies. Rommel's supply lines were a natural target for the British.
The RAF was able to attack Italian convoys crossing the Mediterranean to Rommel because the codebreakers could read both the German Luftwaffe Enigma and the Italian special machine cipher.

PETER HILTON: I could not understand how Rommel failed to realize that we were breaking important signals. I mean, he was a superb general, he was winning, but then he started losing because his supplies were always sunk in the Mediterranean.
NARRATOR: Bletchley Park could pinpoint the location of enemy oil tankers and even know how much gasoline they were carrying. But to keep Ultra safe, it had to look as though the British knew about the convoys from some other source.
RALPH BENNETT: There was an absolutely rigid rule that we could not use Ultra unless first of all an aircraft had been sent out to reconnoiter. Once the Ultra had been proven by the Germans seeing a British airplane looking at the convoy, then you could use it, but not until. They might very well say, "I wonder how they knew it," but fortunately they always deluded themselves by saying it must have been an Italian traitor in the Naples docks.
MANFRED ROMMEL: My father ended his life with the suspicion that there was a gap in the Italian high command through which news escaped and arrived at the British side. But in heaven he must apologize towards the Italians and say, "I was wrong."
NARRATOR: But in the game of intelligence, the Allies had losses as well as gains. Although the German secret service never cracked an Allied cipher machine, Rommel did obtain vital inside information from a spy. The incident began earlier in 1941 when a group of American codebreakers visited Bletchley Park. With America not yet officially at war, the secret services on both sides were nervous about collaborating.
CARL BOYD: Spies are not prone to share a great deal straight away, you know. They - it takes time for spies to warm up with one another, and even British and American spies, they played their cards very close to their chests.
NARRATOR: Although the British worried about the possibility of American security leaks, they began sharing decoded Enigma messages and diplomatic reports about the war. British security fears were justified, for these exchanges soon gave Rommel his own intelligence breakthrough. Reports on the British campaign in North Africa were sent regularly to Washington by the U.S. military attaché in Cairo. The Germans intercepted the messages, but couldn't break the diplomatic code. Then, in September 1941, the Italian secret service broke into the U.S. embassy in Rome and stole the code book used to encipher all U.S. diplomatic messages. The thieves copied the code book and returned it to the safe without anyone knowing. Now Rommel could read all embassy transmissions about the British campaign. Armed with information about British troops and tanks, Rommel launched a bold assault through Libya, pushing the British back 300 miles in 17 days. The news that reached Churchill painted a grim picture of defeat. Now the British needed their own intelligence coup to reverse the disaster. At Bletchley Park, the codebreakers raced to crack the daily rotor settings. Some breaks came in only six to 12 hours. Still, lives might be saved if the operation could be speeded up. The gifted codebreaker Alan Turing had long been intrigued by the idea of building machines to automate the codebreaking process. The Poles had built such a device before the war, but Turing set out to improve on their ideas. Turing's goal was to build a machine that could figure out how the German operators had set up their Enigmas for that day's messages.
Using stock phrases, or cribs, to deduce the rotor settings was the most time-consuming part of the whole codebreaking process.
ANDREW HODGES: Alan Turing's great breakthrough was seeing - that finding out the rotor settings from that crib was something that could be done by a machine, that was the great starting point and brought the whole thing into the modern age.
NARRATOR: Turing's machine was vastly more powerful than the Poles' earlier device. Curiously, Bletchley Park called it the Bomb, perhaps because of the ticking noise it made while operating.
ARTHUR J. LEVENSON: An average Bomb run was about 15 minutes. Occasionally I heard we beat the Germans to the decryption. This happened when A would send B a message and B would almost immediately send back a message, a very short message, which just said, "I can't read you." We would get the solution faster than the other guy could decipher the second sending. And if it was something hot, it'd get out in the field before the German commander got his.
NARRATOR: The Bomb was an array of electromechanical drums that simulated the rotors of the Enigma machines. The drums clicked round letter by letter, testing the thousands of possible Enigma settings - 20 every second - until the correct one had been found.
TONY SALE: Before Turing, the perceived wisdom was, you've just got to go around searching for this one solution which will break a particular message. Turing said no, what you do is you use the mathematical technique of rejecting all things that it couldn't possibly be. So it was a very powerful search

engine, but working in a negative sense in that it rejected millions and millions of possibilities very, very quickly and arrived at the correct answer.
NARRATOR: The Bombs radically sped up the pace of decoding. By the end of the war there were 200 of the devices at six different locations, enabling Bletchley Park to decode 90,000 messages a month.
ANDREW HODGES: The algorithmic process, as we call it now, by which the crib and the cipher text were processed on these mechanical systems, they were the most advanced, most complex processes that had ever been used in the history of the world. I can't think of anything else with its logical and statistical sophistication. It's something you should think of as years and years before its time.
NARRATOR: Meanwhile, in August 1942, Churchill traveled to North Africa, determined to reverse the Allies' fortunes. His first action was to inject fresh blood into the leadership of the 8th Army. He appointed a decisive new general, Bernard Montgomery, to take on Rommel's Africakorps. He knew from Ultra that Rommel was prepared to attack somewhere in Egypt - but where? Montgomery predicted the ridge at Alam Halfa.
RALPH BENNETT: Monty said, looking at the ground, he will go over the Alam Halfa ridge. Some days later we decoded a signal from Rommel saying, I am going to attack on the 30th of September the Alam Halfa ridge, which is exactly what Monty had said. I think from that moment on Monty was so confident of his own intelligence that he couldn't be beaten, he couldn't - he knew everything.
NARRATOR: But Montgomery had another advantage. The Allies finally realized that the Germans were reading U.S. embassy reports on the British campaign, so the embassy changed its diplomatic code. Rommel no longer knew what the enemy was planning. Montgomery was still receiving Ultra from Bletchley Park. Soon, the German forces were under enormous pressure. But some of the decoders began to feel impatient with Montgomery.
PETER HILTON: We felt that Montgomery did not trust the intelligence information that Bletchley Park was providing him with, because we believed in our own arrogant way that we were probably providing a service to the military that no other military had ever had in the history of warfare.
NARRATOR: On the 23rd of October, the British launched its attack at El Alamein.
ARCHIVE RADIO: Our mandate from the Prime Minister is to destroy the Axis forces in North Africa. We're going to finish with this chap Rommel once and for all.
NARRATOR: British intercept stations logged over 300 messages a day in the battle that followed. Bletchley Park knew Rommel's plans, his forces, and his losses. For the first time in the war, an army moved into battle with precise advance knowledge of the enemy. Ultra told Montgomery of Rommel's critical shortages of fuel and tanks. On the evening of the 2nd of November, Rommel signaled Hitler for permission to retreat.
JOHN PRESTWICH: Alamein was marvelous, because you had these desperate messages from Rommel saying, Panzer Army is exhausted, we've enough petrol for 50 kilometers, ammunition is contemptible, and so on, and we have between 11 and 17 operational tanks in the whole of Panzer Army Africa.
NARRATOR: Hitler replied the next day, ordering Rommel not to yield a step, either victory or death. Montgomery read the message within hours. At El Alamein Montgomery's superior forces crushed Rommel. Yet he decided not to pursue the remnants of the retreating German Army.
RALPH BENNETT: We told Monty over and over again how few tanks Rommel had got. So Monty could have wiped Rommel off the face of the earth. Why he didn't do so, why he didn't wipe it off the face of the earth, I simply do not know, nobody else knows.
JOHN PRESTWICH: Why was the Hut 3 information not used? It was so full, I mean that was our exasperation. We were giving Monty every conceivable information about the state of Rommel's troops, the number of operational tanks, which was terribly crucial. I mean, you know, enough - about as many tanks as could be parked on the lawn at the back of this house. In desert warfare, no tanks and you're finished.
RADIO ARCHIVE: This is the BBC Home and Forces program. Here's some excellent news which has come during the past hour from GHQ Cairo. It says, the Axis forces in the western desert after 12 days and nights of ceaseless attacks by our land and air forces are now in full retreat.
BARBARA QUIRK: "Somehow war seems the natural state of affairs, and peace when it comes will take a hell of a lot of getting used to."
NARRATOR: At the time of El Alamein, the U.S. had been at war with Germany for nearly a year. Even before Pearl Harbor, the British Admiralty had been passing decoded U-boat messages to the American Navy. Churchill and Roosevelt knew that the Battle of the Atlantic was crucial and that Ultra gave them a vital edge in the fight against the U-boats. In February 1942, the Admiralty received disastrous news. An abrupt change in the U-boat code plunged Bletchley Park into darkness. They could no longer read the U-

boat signals. Equally serious was an abrupt change in U-boat tactics. German submarines switched from the North Atlantic and began prowling the eastern seaboard of the U.S. There, the marauding U-boats maintained radio silence. When they did transmit, their signals couldn't be decoded. All over the Atlantic, the Allied navies struggled to cope with mounting losses at sea. As the crisis deepened, the naval Enigma team at Bletchley Park worked round the clock to crack the new code, which they called Shark. Since none of the old codebreaking tricks would work, it was obvious that Donitz had somehow drastically changed the Enigma. For the Allies on both sides of the Atlantic, it was a severe blow.

COLIN BURKE: Well, unfortunately the British lost control of the Enigma, and America was left without the kind of vital information needed to protect its convoys. There were an awful lot of protests, and England was very hesitant to tell us that they had lost control of the code.

NARRATOR: Before the blackout, the Admiralty's submarine tracking room had been able to pinpoint U-boats with the help of the navigational positions radioed between Donitz and his crews. Now all they had were rough directional fixes on the signals themselves. Toward the end of 1942, the Allies were losing ships at over four times the rate before the blackout. Finally Bletchley Park figured out what Donitz had done. Though still believing the Allies could never crack Enigma, he was worried about internal security, and ordered the addition of a fourth rotor to the machine. The revolving rotors, with their maze of constantly changing electrical wiring, were the secret of the Enigma. Introducing a fourth one vastly multiplied the number of potential settings. Now the codebreakers would have to build a new type of device to simulate the four-rotor Enigma, and pacify the increasingly impatient Americans.

COLIN BURKE: It got to the point where by mid-1942 the Americans declared that no matter what, they would go their own way and make sure they'd get their own independent capability against the German submarine menace and its code systems. And it became quite touchy as to whether or not the two sides would cooperate.

NARRATOR: Tensions grew when secrets were withheld from an American intelligence officer visiting Bletchley Park. He wrote an angry report home. To resolve the crisis, Bletchley Park's second-in-command traveled to Washington for a meeting with the U.S. Navy. They signed an agreement to resolve concerns about security and to cooperate fully on the breaking of the naval Enigma. As part of the deal, American codebreakers would be sent to Bletchley Park. Together they would take on the challenge of the fourth rotor.

SARAH BARING: What I think bothered us most was the destruction of the merchant shipping and the destruction of the naval ships, and knowing that if only we could break this wretched code, we could save so many lives and sink so many U-boats.

NARRATOR: The first chance to get back into the naval Enigma came when a fresh set of captured U-boat code tables arrived at Bletchley Park, enabling the codebreakers to uncover a critical weakness in the four-rotor system. The German four-rotor Enigma used mainly on submarines had to communicate with other naval stations that used only a three-wheel machine. To solve the problem, the fourth rotor could be set in a special position that allowed the machine to simulate an old fashioned three-rotor Enigma. With the help of the captured tables, the codebreakers worked out the settings of the first three rotors on the Bombs as they had in the past, then simply ran through all 26 positions of the fourth rotor until they found the right one. Soon, the daily settings were on their way to the Admiralty and America. After 10 months in the cold, Bletchley Park was back.

SHAUN WYLIE: The excitement when we got back into the U-boats was terrific. I was on night shift and somebody came running and said, "We're back into the U-boats," and it was the one that meant we were going to be able to go on getting into the U-boats so that was terrific. It wasn't just a one off, it was - we were going to be able to do it steadily. Churchill was told as soon as possible. It was a great moment.

NARRATOR: Once again Bletchley Park could help reroute convoys around the Wolf Packs. Airborne radar and improved escort support helped assure victory in the Battle of the Atlantic. Although only a few of the men and women of Bletchley Park were in a position to appreciate it, the breaking of the naval Enigma was their finest hour. By the spring of 1943, they were decoding dozens of messages a day, and cooperation with the Americans was taken to a new level. The U.S. codebreaking unit was known as Arlington Hall, after its headquarters in northern Virginia. After the war, it would become the National Security Agency, or NSA. Here the first American officers were selected to join the codebreakers at Bletchley Park.

WILLIAM BUNDY: I remember vividly, a group of us were convened in a room there, and the moment we came in they were told, "What you're going to hear today is something you will not discuss, and it

means that you will never be put where you can be captured by the enemy." And I was picked to be the commanding officer of that outfit, and that's how I got to Bletchley Park.
NARRATOR: During their voyage to England, the officers were ordered to tell a bizarre cover story, that they were messenger pigeon experts in the signal corps. This aroused the suspicions of an officer who was checking their identity.
ARTHUR J. LEVENSON: They asked us whether we'd had the Army general classification test, they said they couldn't find our scores on our records. They said, would you mind taking the test, and we said no, we don't mind. There were five of us, and we took the test, and this sergeant graded them, and he came running up, he says, "Holy mackerel. What scores! You guys ought to be in intelligence!" I don't think I'd ever met an Englishman in my life until that point. I had been full of stereotypes about the English, you know, they're distant and have no sense of humor, and these were the most outgoing, wonderful people. Fed us when it was quite a sacrifice, just enough screwballs to be real fun.
LORD BRIGGS: It was the first time I'd ever been involved in my life in any serious discussion, both either about war or politics with an American. It was there that I learnt for the first time to drink tomato juice, it was the first experience I had with American coffee and American bacon, so that in a way America was introduced to me through this Bletchley prelude.
NARRATOR: The Americans quickly settled into life at Bletchley Park. The only serious dispute arose when the British challenged the Americans to a game of rounders, the British version of baseball.
BARBARA EACHUS: We said of course, we were delighted, you know, our honored allies. So the Americans came and we showed them how they could play with - they said what, no baseball bat? We said no, we just use this broom handle. So they said fine. And we played. It was a lovely day. We all played well. And at the end of the game, we all sort of clapped each other on the back and the Americans said well, "We're sorry we beat you," and the British captain said, "I'm sorry we beat you." And that was a little bit of an incident, because the Americans said they thought they'd won, and we said we knew we'd won. And they said, "Well what rules do you play by?" And we said, "Our rules."
NARRATOR: As the Americans adapted to their new life, their colleagues told them about a mysterious and daunting codebreaking problem. They knew that in addition to Enigma, the Germans sometimes used another completely different kind of cipher machine.
TONY SALE: Now we knew nothing about this cipher machine, it was kept completely secret by the Germans, and we first began to intercept radio transmissions in 1940. It was actually a group of policemen on the south coast of England. They were listening for German agent transmissions from within the U.K. Of course there weren't any because we'd captured all the agents, but they were still listening for these and they heard these weird signals. And they sent them to Bletchley Park.
NARRATOR: At first, the decoders puzzled over the origin of the strange signals. Hitler had demanded a cipher machine for the German high command that was faster and even more secure than the Enigma. His experts devised a coding system based on the teleprinter machine. Teleprinters operated on a simple, universal binary code that was widely known. But the Germans connected the teleprinter to a machine that cunningly exploited the teleprinter language itself to produce a complex code. The secret German coding machine was called the Lorenz. To scramble a message the Lorenz used 12 rotors - not just the three or four of the Enigma.
DONALD MICHIE: The Lorenz machine transmits a string of letters, each one of which is actually a mix of the real letter of the real message and a piece of machine crafted gobbledygook, that machine being of diabolically complex craftiness. So at the end of it, what comes out and goes over the ether and is transmitted, is a single string of total gobbledygook.
NARRATOR: The Lorenz relied on a mathematical system called "modulo two addition." This allowed the string of meaningless letters added to the message at one end to be removed at the other by a similar math calculation.
TONY SALE: The operator presses a key on his teleprinter, that generates an electrical signal, the Lorenz machine then adds an obscuring character to this signal and the result is then transmitted. At the other end of the link another Lorenz machine set to exactly the same configuration regenerates exactly the same obscuring character, adds it back to the cipher text, and by the magic of modulo two arithmetic they cancel out and leave you with the plain text.
NARRATOR: The security of the Lorenz depended on the fact that it was adding a string of random letters to hide the real message.

TONY SALE: But because it's a machine, it can't generate a completely random set of letters. It's what's known as pseudo random. Unfortunately for the Germans it was more pseudo than random, and that's how it was broken.
NARRATOR: Bletchley Park gave the mysterious code the name FISH. They worked out that fish was based on teleprinter language. How to strip off the obscuring code was anybody's guess. But on the 30th of August, 1941, a lazy German operator gave the whole game away.
TONY SALE: When he got to the end of keying in this nearly 4,000 character message by hand, the operator at the receiving end sent back in German the equivalent of, "Didn't get that, send it again." And then like idiots they both put their Lorenz cipher machines back to the same start position, and then he began to key this long message again.
NARRATOR: When the operator began to encode the same message a second time, he grew impatient and abbreviated parts of it. The resulting slight changes enabled the codebreakers to strip off the random letters that were cloaking the message.
PETER HILTON: For me the real excitement was this business of getting these two texts out of one sequence of gibberish, it was marvelous. Never, never met anything that was quite as exciting. Especially since you knew that these were vital messages.
NARRATOR: Now that they had decoded the message, could they use it to figure out exactly how the Lorenz machine worked? For the next two months, the codebreakers hunted laboriously for patterns in the endless strings of obscuring letters. Eventually they were able to reconstruct the precise mechanics of the Lorenz - a machine they had never seen. They even built their own replica. Since it was used to crack the mysterious Fish code, they called the replica Tunny, after a fish in the tuna family. Once the Lorenz settings were found, Tunny could turn the messages into plain German. Despite the advances in understanding Fish, it still took at least a month to decode a single message, and by then the information was generally useless.
LORD JENKINS: It was a curious life, it involved mental gymnastics and it could be, could be very wearing, particularly if you didn't succeed. I mean, you could spend nights in which you got nowhere at all. You didn't get a single break, you just tried, played around, played around through this bleak long night with total frustration, and your brain felt literally raw, your psyche or whatever it is felt frustrated, but your brain always literally felt raw at the end of it.
NARRATOR: But the whole process was about to be speeded up. At the post office research station in London, a brilliant young telephone engineer hit upon the idea of an electronic machine that would automate the hunt for the Fish settings. The machine would be nothing less than the world's first programmable computer.
THOMAS H. FLOWERS: I tried to tell Bletchley Park what my ideas were, but you must understand the technology that I was using was then only just known to very few people in the whole world.
NARRATOR: Though the codebreakers were skeptical, Flowers was convinced the answer lay in vacuum tubes - hundreds of them.
TONY SALE: Tommy Flowers started in March 1943 with a blank sheet of paper, never been done before. I mean Flowers was thinking of a machine with 1,500 valves in it. The biggest machine ever at that time had 150 valves in it, so this was an enormous leap into the dark, but Flowers was convinced he could make it work - nobody else was but he was - and so he started more or less off his own bat.
THOMAS H. FLOWERS: We just told people to do things. We had the power, we had the authority to tell anybody - we had the first priority in the whole country for everything, and we could just tell people what we wanted and not tell them what it was for.
NARRATOR: Over Christmas 1943, Tommy Flowers installed the world's first programmable computer at Bletchley Park. Eventually ten more were built, all dedicated to analyzing the secret messages of the German high command. They were given the name Colossus. Colossus could read a coded message at high speed and then search for the settings of the Lorenz code wheels. It could accomplish this in minutes instead of a month.
TONY SALE: Tommy Flowers realized that it was possible to read paper tape optically at very high speed, and this is going at 5,000 characters a second, 30 miles an hour the tape goes through there. And it's quite incredible that it can actually read information at that speed.
THOMAS H. FLOWERS: In fact, we did a test on how fast we could drive it before the tape broke, and we got up to nearly 60 miles an hour, so we decided that was a bit - when it did break it went all over the place, it just disintegrated.

NARRATOR: Colossus began operating five months before D-Day, the critical invasion of France in June1944 that would turn the tide against Hitler. Tanks and guns choked every main road and street in southern England. The Allies prepared an elaborate deception. They set out to trick the Germans into thinking that the attack on Normandy was simply a diversion. Double agents in Britain relayed the false information to Berlin, but only the codebreakers could tell if the deception was working.
PETER CALVOCORESSI: The Germans were deceived for a very long time, far more than we expected and far more successfully. But we also got a bonus, if you like. That is, we knew they were deceived, because from Ultra we could see that they were not moving troops into Normandy, they had to say to themselves, they'll pop over to Calais. The Germans were not only deceived, they were known to be deceived.
NARRATOR: It was an enormous subterfuge and an even bigger gamble. Around the clock, the Allies searched for the merest hint of German suspicion. The invasion was poised to strike. But then, a vital message was decoded at Bletchley Park.
ARTHUR J. LEVENSON: Just before D-Day, Marshal Rommel, the desert fox, was appointed inspector general of the western defenses, and he sent this enormously long message, very detailed description of the western defenses, where each unit was located and what equipment they had. It was a - it was 70,000 letters, which was read.
NARRATOR: When Bletchley Park decoded Rommel's message, it contained alarming news. German tanks were massing at the exact spot where American troops were about to parachute into Normandy.
ARTHUR J. LEVENSON: They were going to drop the - one of the airborne divisions right on top of a German tank division. They would have been massacred. They changed it.
NARRATOR: It was June 4th, 1944. Reassured by the codebreakers that all was well, the massive army began to move forward. Then came a discouraging setback.
PAT BING: We went on duty that night and they said, "Well, tonight is the invasion and they're going across." And so we slaved away. Well, of course as everybody knows, by about four o'clock in the morning, the weather was so bad they had to bring them all back. Which of course was bad luck for us because they then came and said, well you can't go walking about Bletchley when you know that the invasion's going to be tomorrow night, so we just had to stay there.
NARRATOR: Twenty-four hours later, the Allies launched the biggest military invasion in history.
SARAH BARING: We had dinner and we came out at eleven o'clock, and I suddenly started to hear a hum and it got louder and louder and louder, and I knew what it was. And about ten minutes later the sky was black with aircraft towing gliders, and my friend said, I wonder what that is, and I said, I haven't the faintest idea.
WILLIAM BUNDY: And about three o'clock, I think it was, suddenly there was a real rustle and very shortly the word spread that there had been German traffic saying that paratroopers were dropping all over the place. So we knew, we knew this was it.
NARRATOR: The decoded messages showed that the deception had worked. Hitler's troops were split between Normandy and Calais and were unable to counter the onslaught. Over half the German forces had remained in the northeast, awaiting an attack that never came. At Bletchley Park, those who knew about the invasion weren't allowed to leave for 48 hours. Even now, nobody was taking any chances.
PAT BING: We staggered out feeling rather the worse for wear, but knew it was then general knowledge, and went home, and my lady I was billeted on said to me, where the bloody hell have you been? And I said, well I've been working. She said, "Well you've missed all the fun." And I said, "What fun?" And she said, "Well there was the invasion, it's been on the radio" - 'cause no television - it's been on the radio. I said, "Oh lovely," you know, and went to bed.
BARBARA QUIRK: "Tuesday, 6th of June, 1944, invasion began. 10 a.m. breakfast, letter from Maureen, spent morning washing and ironing, on at four, life quite hectic. Feel somewhat anticlimax-y now the second front has begun. Not a bad day, really."
NARRATOR: It had not been a bad day for the codebreakers either. They had accurately foretold the position of all but two of the 62 German divisions. Enigma and Lorenz messages were read throughout the D-Day operation. By the end of the war, they had handled at least 63 million characters of high level code between Hitler and his generals. In the months that followed, Bletchley Park would continue to chronicle the disintegration of Nazi Germany - right until the end of the war. Finally, at the cost of at least 50 million lives, the Second World War came to an end.
LORD BRIGGS: When the final signal came through from Donitz surrendering, it was in clear and not in code, and that was extremely interesting because you felt the war was then really over. When messages did

begin to come through in clear, then all the secrets of the war really were beginning to fade into history already.
NARRATOR: In the roll call of those who had brought about victory, the codebreakers of Bletchley Park would never be mentioned. The operations there were to stay a secret for the next 30 years. Eight of the ten Colossus machines were destroyed. The remaining two were moved to British secret service headquarters, where they may have played a significant part in the codebreaking operations of the Cold War. In fact, the Russian military had developed a code that was similar to the high command's Fish code. So the techniques invented at Bletchley Park were still to prove vital in a very different kind of conflict. In 1960, the order finally came to destroy the last two Colossus machines.
THOMAS H. FLOWERS: That was a terrible mistake. I was instructed to destroy all the records which I did. I took all the drawings and plans and all the information about Colossus on paper and put it in the boiler fire, saw it burn.
NARRATOR: Tommy Flowers returned to the post office and was forgotten. In all the secrecy, Colossus never received recognition as the world's first programmable computer. Instead, that honor was to go to the American Eniac. As for the codebreakers, they all dispersed, some back to universities and others into the fledgling computer industry. A few stayed on in the British secret service, while some of the Americans returned to Arlington Hall. The most innovative thinker of all, the man whose inventiveness had been at the center of Bletchley Park's success, died tragically. In 1954, Alan Turing took his own life after being persecuted as a security risk because he was gay.
DONALD MICHIE: Alan Turing is one of the figures of the century. The world of computing and now the world of the Internet stems from Alan Turing's fundamental ideas. There were other great men in Bletchley Park, but in the long, long hall of history, I think Turing's name will probably be the number one in terms of consequence for mankind.
NARRATOR: Apart from the Atom Bomb, there was no greater secret in World War II than the work of the codebreakers of Bletchley Park. Their breakthroughs gave the Allies a vital edge in the U-boat war, the tank battles against Rommel, and the D-Day invasion. But their impact was felt far beyond the battlefield. Eavesdropping and decryption won a new prominence in the minds of politicians as well as generals. The transatlantic alliance, that took its first hesitant steps at Bletchley Park, would mature and prove critical during the Cold War. And the roots of today's computer era trace back directly to the dazzling inventiveness of Turing, Flowers, and their wartime colleagues. In the end, though, Bletchley Park's greatest achievement lay not in broken ciphers but in the hundreds of thousands, perhaps millions, of lives it saved.
TONY SALE: Historians generally agree that it shortened the war by two years. Bletchley Park didn't win the war, that was won by people with guns and bullets and things out in the field, but I think Bletchley Park is a great exemplar, particularly to the younger generation now, of brains over bullets. You can defeat an enemy intellectually, and that was shown here.
The World Wide Web relies on more sophisticated codes than were used in all of World War II. On NOVA's Website, find out how cryptography affects you today more than you may think.

Next time on NOVA: they risked it all in a perilous flight to the finish.
It was a very important secret, and it paid off.
Now, get the real story behind the race to fly faster than sound. ■