MODERN MARVELS: CODES NETWORK: THE HISTORY CHANNEL Writer/Producer/Director: Adrian Maher Date: April 6, 2001	
TEASE	
	CAESAR ALTERED HIS ALPHABET. THE NAZIS HAD ENIGMA. THE MODERN AGE HAS COMPUTERS AND DIGITAL ENCRYPTION. THE ATTEMPTS TO MAKE AND BREAK THESE SECRET METHODS OF SCRAMBLED COMMUNICATION HAVE CHANGED THE COURSE OF HISTORY..…NOW “CODES” ON MODERN MARVELS.
ACT ONE	
	MANILA, THE PHILLIPINES, JANUARY, 6, 1995. WHEN POLICE RESPONDED TO AN APARTMENT FIRE THEY FOUND A TOSHIBA LAPTOP AMID A BATCH OF CHEMICALS AND BOMB-MAKING MATERIALS. AN OPEN FILE ON THE LAPTOP REVEALED A PLAN TO SIMULTANEOUSLY BOMB 12 U.S. AIRLINERS OVER THE PACIFIC. THE POTENTIAL DEATH TOLL - 4,000 PASSENGERS. SEVERAL OTHER FILES USED ENCRYPTION SOFTWARE THAT SCRAMBLED THE WRITINGS IN SECRET CODE. THE PHILIPPINE POLICE DECODED SOME OF THE FILES USING A SPECIAL COMPUTER PROGRAM AND UNCOVERED A LIST OF BOMB-MAKING RECIPES. ALL THE EVIDENCE POINTED TO THE MOST HUNTED TERRORIST IN THE WORLD: RAMZI YOUSEF - WANTED FOR HIS INVOLVEMENT IN THE WORLD TRADE CENTER BOMBING. YOUSEF’S PLOTS WERE STOPPED AND HE WAS IN U.S. CUSTODY WITHIN SIX WEEKS.
	IT WAS A MAJOR VICTORY FOR

	INTERNATIONAL LAW ENFORCEMENT AND REVEALED THE IMPORTANCE OF CRYPTOLOGY - THE SCIENCE OF MAKING AND BREAKING SECRET CODES.
	TO TRACE THE DEVELOPMENT OF CODES IS TO UNCOVER THE VERY FABRIC OF CIVILIZATION. ONCE A CULTURE REACHES A LEVEL OF SOPHISTICATION IN LITERACY, SCIENCE AND LANGUAGE, THE DEMAND FOR SECRET SYMBOLIC COMMUNICATION FLOURISHES.
	Dr. David Hatch, Director of the Center for Cryptologic History (53160) 01:01:11 I think codes go back, probably as far as there is language. People had something to keep secret. They needed to find some way to scramble it.
	FOR CENTURIES CODES HAVE BEEN CONTROLLED BY GOVERNMENTS - EMPLOYED IN WAR, APPLIED IN DIPLOMACY AND USED IN ESPIONAGE. BUT WITH MODERN TECHNOLOGY, THE USE OF CODES BY INDIVIDUALS HAS EXPLODED, ENRICHING CRYPTOLOGY AND EMPOWERING CITIZENS. A COMMUNICATIONS BOOM HAS HEIGHTENED THE NEED FOR CODES TO KEEP INFORMATION PRIVATE - ON THE INTERNET, AT A-T-M'S, AND IN MEDICAL OFFICES. TODAY'S COMPLEX CODES ARE THE RESULT OF A HISTORIC SEESAW BATTLE BETWEEN CODEMAKERS AND CODEBREAKERS THAT HAS PUSHED THE VERY BOUNDARIES OF SCIENCE.
	THE EARLIEST KNOWN CODE WAS AN INSCRIPTION CARVED INTO ROCK BY AN EGYPTIAN SCRIBE IN 1900 B.C. IT WAS AN ATTEMPT TO DEMONSTRATE WIDER

	KNOWLEDGE BY DRESSING UP THE WRITING. ORDINARY HIEROGLYPHICS WERE REPLACED WITH UNUSUAL SYMBOLS THAT TOLD THE STORY OF THE WRITER'S MASTER, KHNUMHOTEP II. ANOTHER EARLY CODE WAS USED FOR SECRECY. A TINY ENCIPHERED TABLET FOUND ON THE BANKS OF THE TIGRIS RIVER, DATING FROM 1500 B.C., CONTAINED A HIDDEN FORMULA FOR GLAZING POTTERY. AND THE ANCIENT GREEKS CREATED THEIR OWN INVENTIVE CODING METHODS.
	David Kahn (53169) 01:05:06 One of the subordinates of a Persian monarch thought that it might be time to revolt, and he had an agent in the court of Darius the Great, and this agent sent a message to this man saying it's now time to revolt….he shaved the head of one of his slaves, and tattooed on the head the word "revolt," and waited for the hair to grow and sent the slave down to this man's palace. When the man got the slave, he shaved the head, saw the word "revolt" and realized that this was the time, and he did revolt successfully.
	IN SPARTA, A NEW INSTRUMENT TO ENCIPHER MESSAGES BETWEEN LEGIONS WAS USED. IT WAS CALLED A SKYTALE (SITILY).
Illustration	David Hatch (53160) 01:02:45 A cloth was wrapped around a stick and the message written down the side. Wrapped around the stick, the message could be read. Unwrapped, it was scrambled. The message was sent from general to general unwrapped. The generals would have a stick of the appropriate length, could wrap the cloth around it and read the message.

	EVERY CODE HAD A KEY, A SECRET METHOD OF SCRAMBLING AND UNSCRAMBLING MESSAGES USED BY SENDER AND RECEIVER. JULIUS CAESAR ENCIPHERED HIS MILITARY COMMUNICATIONS USING A KEY THAT EMPLOYED AN ALTERNATIVE ALPHABET BY MOVING EACH LETTER THREE SPACES TO THE RIGHT. BUT WITH THE COLLAPSE OF THE ROMAN EMPIRE IN 500 A.D., EUROPEAN CRYPTOLOGY ENTERED A DARK AGE THAT WOULD LAST FOR 1,000 YEARS.
	BUT ANOTHER CIVILIZATION WAS RISING IN THE EAST. BY 900 A.D., ARAB SOCIETY WAS ONE OF THE MOST LITERATE CULTURES IN THE WORLD AND THE STUDY OF CODES FLOURISHED. THE ARABS WERE THE FIRST TO RECORD THE METHODS OF TRANSPOSITION, THE SCRAMBLING OF LETTERS, AS WELL AS SUBSTITUTION, THE REPLACEMENT OF LETTERS WITH NUMBERS AND SYMBOLS. THEY WERE THE FIRST TO OUTLINE SPECIFIC TECHNIQUES OF CODEBREAKING THAT INVOLVED MATHEMATICAL OR FREQUENCY ANALYSIS.
	David Kahn (53169) 01:11:50 The Arabs were very interested in letter studies. … they counted the number of times a character, such as Aleph, appeared in the Koran and they discovered which letters began words frequently…they used this information, a statistical source, to learn how to break codes…The most frequent coded letter represents the most frequent plain-text letter, and that's how you begin to solve a code, and they were the first to do this.
	WITH THE RENAISSANCE,

Illustration	CRYPTOLOGY HAD A REBIRTH IN EUROPE. IN 1466, AN ITALIAN ARCHITECT, LEON ALBERTI, DEVELOPED THE GREATEST CRYPTOLOGIC INVENTION IN A THOUSAND YEARS AT THE URGING OF THE VATICAN. IT WAS A SYSTEM OF ROTATING CIPHER DISCS WITH TWO RINGS OF LETTERS AND SEVERAL NUMBERS. BY SCRAMBLING SO MANY LETTERS RANDOMLY, IT WAS THE FIRST TO CHALLENGE THE ARAB CODEBREAKING METHOD OF FREQUENCY ANALYSIS.
	David Kahn (53169) 01:14:06 Previous systems just replaced A with D or A with Q….only one at a time. The Alberti cipher discs used a disc in which these letter combinations could be changed from time to time, and as a consequence, A would be represented not by only one letter, but by many letters. This was called poly-alphabetic - many alphabet substitution. And it was the basis for many modern cipher systems.
Illustration	A FRENCH DIPLOMAT, BLAISE DE VIGENERE, IMPROVED THE ALBERTI SYSTEM IN 1586 BY CREATING A GRID OF 26 CIPHER ALPHABETS, EACH SHIFTED ONE OVER FROM THE LAST. BY USE OF A KEYWORD, ENCODING AND DECODING COMMUNICATIONS USING VIGENERE'S SQUARE COULD BE CALCULATED ON A SHEET OF PAPER INSTEAD OF HAVING TO CARRY A DISC.
	UNFORTUNATELY, MARY QUEEN OF SCOTS DID NOT EMPLOY THIS NEW DEVELOPMENT. BEGINNING IN 1568, MARY WAS IMPRISONED BY HER COUSIN, QUEEN ELIZABETH I OF ENGLAND. IN 1586, A GROUP OF

Illustration	CATHOLICS SOUGHT TO RESCUE MARY AND PUT HER ON ENGLAND'S THRONE AFTER ASSASSINATING ELIZABETH. HER RESCUERS COMMUNICATED WITH MARY THROUGH SECRET CODED LETTERS.
	David Hatch (53160) 01:08:40 Her great mistake was in thinking that her cipher system was secure. It was actually being read by Queen Elizabeth's codebreakers and everything about the plot was known, and when it reached a certain critical point, Queen Elizabeth called a halt to it and sentenced Mary, Queen of Scots to death.
	BY THE 1700s, EACH EUROPEAN POWER HAD ITS OWN "BLACK CHAMBER," A NERVE CENTER FOR DECIPHERING MESSAGES AND GATHERING INTELLIGENCE.
	BUT THE REAL REVOLUTION IN CRYPTOLOGY WAS JUST AHEAD.
	David Hatch (53160) 01:10:13 Telegraph, for the first time, made it possible to send messages quickly over long distances. In fact it made the United States a continental power by increasing its communications power. It also raised the necessity for cryptology.
	IN 1844, SAMUEL MORSE INVENTED MORSE CODE, A SERIES OF ELECTRICAL DOTS AND DASHES TO COMMUNICATE OVER THE TELEGRAPH. BECAUSE THE CODE WAS PUBLIC, AND MESSAGES COULD BE EASILY INTERCEPTED, THE NEED FOR NEW SECRET CODES BECAME ACUTE. BUT THE TELEGRAPH PALED IN COMPARISON TO THE COMMUNICATION INDUSTRY'S NEXT SCIENTIFIC DEVELOPMENT - ONE THAT

	REVOLUTIONIZED CODES AND WAS USED WITH MURDEROUS IMPACT IN THE TWENTIETH CENTURY.
	FACTOID: SECRET SIGNALS USING FLAGS WERE USED EXTENSIVELY ON THE BATTLEFIELD IN THE AMERICAN CIVIL WAR.
	CODES WILL RETURN ON MODERN MARVELS.
ACT TWO	
	WE NOW RETURN TO CODES ON MODERN MARVELS.
	AT THE DAWN OF THE TWENTIETH CENTURY, AN ITALIAN PHYSICIST, GUGLIEMO MARCONI, CHANGED THE WORLD OF CODES FOREVER. MARCONI'S INVENTION HARNESSED RADIO WAVES AS A NEW METHOD OF COMMUNICATION. THE RESULT WAS AN INSTANTANEOUS TRANSMISSION OF MESSAGES ACROSS LONG DISTANCES.
	David Kahn (53169) 01:22:44 The invention of the radio was the most important single event in the history of codes and ciphers…Radio had the great effect of facilitating communications - you don't have to lay wire or anything like that, you can just go out with a radio post and communicate, but it has the great disadvantage of turning over to the enemy every message that you send, so this means you have to put into code every message that you send…so it stimulated enormously the great growth of codes and ciphers.
	THE RAMIFICATIONS OF THIS NEW INVENTION WERE NOT LOST UPON THE GENERALS. RADIO ALLOWED QUICK COMMUNICATION WITH FIELD DIVISIONS AND A MORE RAPID, MOBILE FORM OF WARFARE.

	RADIO MESSAGES WERE ENCIPHERED AND SENT IN MORSE CODE ACROSS THE AIRWAVES. BUT RADIO TRANSMISSION REVEALED EVERY CRYPTOGRAM IT CONVEYED. IT FURNISHED A CONSTANT AND MASSIVE STREAM OF INTERCEPTS TO THE ENEMY. WITH THE OUTBREAK OF WORLD WAR I, THE NEED FOR NEW CODES AND CODEBREAKERS SHARPLY ESCALATED. A GLOBAL BATTLE OF SECRET COMMUNICATIONS HAD BEGUN. ON AUGUST 5, 1914, BRITISH DIVERS FROM THE SHIP TELCONIA SEVERED GERMAN CABLE LINES IN THE NORTH ATLANTIC.
	Stephen Budiansky - Author: Battle of Wits (53145) 04:24:59 It appears their idea was simply to make things more difficult for the Germans, but it had the payoff of forcing a great deal of traffic that would have gone by cable, onto radio. And so it resulted in really a flood of intercepts coming in that otherwise wouldn't have been available.
	ONCE INTERCEPTED THEY WERE SENT TO ROOM 40, THE CRYPTANALYSIS SECTION OF THE BRITISH ADMIRALTY.
	David Hatch (53160) 01:18:06 Room 40 might be the prototype of modern cryptanalytic organizations…they recruited mathematicians, linguists, chess masters, anybody who was good at puzzle-solving.
	IN SEPTEMBER, 1914, BRITAIN RECEIVED ONE OF THE GREATEST GIFTS IN THE HISTORY OF CRYPTOLOGY. HER ALLIES, THE RUSSIANS, CAPTURED THE GERMAN CRUISER MAGDEBURG IN THE

	BALTIC AND A BOOK OF GERMANY'S MAIN NAVAL CODE. THEY PROMPTLY TURNED THE CODE BOOK OVER TO ROOM 40 ALLOWING BRITAIN TO BREAK GERMAN NAVAL MESSAGES AND BOTTLE-UP GERMANY'S BATTLESHIPS FOR THE DURATION OF THE WAR. CODEBREAKING HAD TRANSFORMED MODERN COMBAT.
	Stephen Budiansky (53145) 04:28:06 Being able to read the German naval signals, often, instantaneously was something that simply hadn't happened before in warfare.
	ON THE EASTERN FRONT, CRYPTOGRAPHY OR LACK OF IT, LED TO ONE OF THE MOST CRITICAL BATTLES IN WORLD WAR I. IN LATE AUGUST, 1914, THE RUSSIANS SENT TWO ARMIES INTO EAST PRUSSIA IN A PINCER MOVEMENT TO TRAP THE GERMANS NEAR THE VILLAGE OF TANNENBURG. THE GERMANS WERE OUTMANNED BUT HAD THE ADVANTAGE OF LISTENING IN ON RUSSIAN RADIO COMMUNICATIONS. DUE TO THE RUSSIANS' RUDIMENTARY AND DISORGANIZED CODING SYSTEM, INTERCEPTS TOLD THE GERMANS THAT THE RUSSIAN'S SOUTHERN ARMY WAS MOVING FASTER THAN IT'S NORTHERN FORCE. THE GERMANS WHEELED AND DESTROYED THE RUSSIAN SOUTHERN ARMY, CAPTURING 100,000 PRISONERS, WITH AN ESTIMATED 30,000 DEAD OR MISSING.
	David Kahn (53169) 01:23:41 This was the first great defeat of the Russians in the war, and it started them on their long slide into ruin and revolution.

	// 01:26:07 The Russians did not at World War I, have a good cipher system, and in part, they lost the war because of it.
	BUT THE GREATEST CODEBREAKING EVENT IN THE HISTORY OF CRYPTOLOGY BEGAN ON JANUARY 17, 1917. THE BRITISH INTERCEPTED A TELEGRAM THAT WAS ENCRYPTED WITH THE HIGHEST GERMAN DIPLOMATIC CODE, 0075. IT WAS A MIND-NUMBING SYSTEM OF 10,000 WORDS AND PHRASES ATTACHED TO A THOUSAND NUMERICAL CODEGROUPS. THE SECRET MESSAGE WAS FROM THE GERMAN FOREIGN MINISTER, ARTHUR ZIMMERMANN TO HIS AMBASSADOR IN WASHINGTON, JOHANN VON BERNSTORFF, FOR RELAY TO GERMANY'S AMBASSADOR TO MEXICO, HEINRICH VON ECKHARDT. THE TELEGRAM WOULD BE DECIPHERED THERE AND SENT TO MEXICO'S PRESIDENT, VENUSTIANO CARRANZA.
	David Hatch (53160) 01:26:28 It was sent from Berlin to Washington encrypted on the American undersea telegraph cable. The British intercepted it there, recognized its importance….It was in a new diplomatic system which the British had not yet broken.
	AFTER RECEIVING THE MESSAGE IN THE NEW 0075 CODE, VON BERNSTORFF'S OFFICE IN WASHINGTON THEN MADE A FATAL MISTAKE.
	David Hatch (53160) 01:26:28 In Washington, they took this

	telegram out of the new diplomatic code book, re-encrypted it in the old diplomatic code book, and sent it to Mexico City on the telegraph.
	BUT THE BRITISH HAD ALREADY BROKEN THE OLD CODE.
	The British intercepted that version, as well, had versions to compare..…perhaps the silliest, most tragic error that a cryptographer can make.
	BRITISH CRYPTANALYSTS BEGAN TO DECIPHER THE MESSAGE IN THE OLD CODE, IN PAINSTAKING CHUNKS, CONSTRUCTING PATTERNS USING PENCIL AND PAPER. WITHIN DAYS, THEY HAD IT.
	AS THE MEANING OF ZIMMERMANN'S SECRET MESSAGE BEGAN TO EMERGE, THE IMPORT WAS EXPLOSIVE. DESPITE THE SINKING OF THE AMERICAN OCEAN LINER LUSITANIA BY THE GERMANS IN 1915, AMERICA MAINTAINED ITS NEUTRALITY WITH THE PROMISE OF GERMAN RESTRICTIONS ON ITS U-BOATS. THE ZIMMERMANN TELEGRAM OUTLINED GERMANY'S INTENT TO RESUME UNRESTRICTED SUBMARINE WARFARE ON FEBRUARY 1, 1917, AS A MEANS TO STRANGLE BRITAIN. TO KEEP AMERICA AT BAY, ZIMMERMANN PROPOSED THAT MEXICO INVADE THE UNITED STATES AND RECLAIM TEXAS, NEW MEXICO AND ARIZONA. GERMANY ALSO ASKED MEXICO TO PERSUADE JAPAN TO ATTACK AMERICA. THE ACTIONS WOULD BE BACKED WITH GERMAN MILITARY AND FINANCIAL AID.
	THE BRITISH ADMIRALTY WAS DESPERATE TO GET THE DECIPHERED MESSAGE TO THE

	AMERICANS WITHOUT ALERTING THE GERMANS THAT THEIR CODE HAD BEEN BROKEN. A BRITISH AGENT WAS ABLE TO INFILTRATE THE MEXICAN TELEGRAPH OFFICE AND RETRIEVE A DECIPHERED COPY OF THE MESSAGE TO MEXICO'S PRESIDENT. ONCE THEY HAD THEIR COVER OF A SUPPOSED LEAK IN MEXICO, THE BRITISH APPROACHED THE AMERICANS AND REVEALED THE TELEGRAM.
	David Kahn (53170) 02:02:51 The whole country blew up. Everybody was incensed. Formerly only the East Coast was concerned, now suddenly the whole Midwest was worried about Mexico….. and six weeks after this message was deciphered, the United States declared war on Germany. So, it was probably the most significant event in code-breaking history and certainly in intelligence history.
	David Hatch (53160) 01:23:42 What the Zimmermann telegram did was convince the entire country that Germany was a national enemy. And a few months later, when Woodrow Wilson asked for a declaration of war, he had a united and angry country behind him ready to go to war against the Germans.
	A SINGLE BREAKTHROUGH BY THE CRYPTANALYSTS IN ROOM 40 HAD SUCCEEDED WHERE THREE YEARS OF INTENSIVE DIPLOMACY HAD FAILED.
	CODEBREAKING WOULD PLAY AN EVEN GREATER ROLE IN CRYPTOLOGY'S GOLDEN AGE, WORLD WAR II.
	FACTOID: AS A RESULT OF THE RUSSIANS DISASTROUS CODING EXPERIENCES IN WORLD WAR I,

	THE SOVIET UNION DEVELOPED ONE OF THE WORLD'S BEST UNBREAKABLE CODING SYSTEMS.
	CODES WILL RETURN ON MODERN MARVELS.
ACT THREE	
	WE NOW RETURN TO CODES ON MODERN MARVELS.
	AT THE END OF WORLD WAR I, THE POWER OF THE CODEBREAKERS OVER THE CODEMAKERS SEEMED OBVIOUS. BUT BY 1917, AMERICAN INVENTOR EDWARD HEBERN CONCEIVED THE FIRST MODEL OF AN ELECTRICAL MACHINE MADE WITH A WIRED ROTOR OF LETTERS ATTACHED TO A KEYBOARD. ONE YEAR LATER, A GERMAN ELECTRICAL ENGINEER, ARTHUR SCHERBIUS, INDEPENDENTLY CREATED AN ELECTRICAL ENCRYPTION MACHINE SIMILAR TO HEBERN'S WITH SEVERAL ROTORS. THE INVENTIONS REVOLUTIONIZED CRYPTOGRAPHY BY MECHANIZING THE PRODUCTION OF CODES WITH MILLIONS OF POTENTIAL VARIATIONS.
Animation	David Kahn (53172) 04:02:55 Imagine a hockey puck, 26 electrical contacts on one side, 26 electrical contacts on the other side, wired at random. You shoot an electrical current through into A. It comes out Q, lights up a letter. Now this hockey puck turns one space. You shoot a current in again at A. Now it's gonna come out at X. And this continues to turn until you go through all 26 revolutions. And then, instead of just having one cipher machine, one cipher wheel next to another, you have several rotors next to each other.
	BY THE MID-1920s, SCHERBIUS WAS

	MASS-PRODUCING HIS NEW MODEL, CALLED ENIGMA. OVER THE NEXT TWO DECADES HE WOULD SELL MORE THAN 30,000 UNITS TO THE GERMAN MILITARY THAT VIEWED IT AS A GODSEND.
	MEANWHILE, THE CRYPTOLOGY OFFICES OF THE ALLIES HAD DWINDLED IN PERSONNEL AND QUALITY. BUT POLAND, BECAUSE OF ITS GEOGRAPHICAL VULNERABILITY BETWEEN GERMANY AND RUSSIA, WAS DESPERATE FOR INTELLIGENCE.
	THE POLES SET UP A WORLD-LEADING CRYPTANALYST BUREAU AND HIRED A GROUP OF BRILLIANT MATHEMATICIANS. ONE OF THEM WAS 23-YEAR-OLD MARIAN REJEWSKY. (RAY-EF-SKI)
	Stephen Budiansky (53142) 01:11:23 What Rejewsky realized was that if you have a machine that's based on rotors, there's certain mathematical relationships between the way it enciphers a letter in one position, and the way it enciphers a letter in the next position in sequence. // 01:09:17 I mean even today it's an astonishing accomplishment, of what he did, was able to reconstruct the wiring of the rotors of an Enigma machine…without ever seeing one.
	IN BUILDING HIS OWN MODEL OF THE GERMAN MILITARY ENIGMA ALL REJEWSKI HAD WAS A COMMERCIAL VERSION OF ENIGMA, AND HIS EXTRAORDINARY MATH SKILLS. AT THE TIME, ONLY A FEW HUNDRED GERMAN MILITARY ENIGMA UNITS EXISTED AND ALL WERE KEPT UNDER TIGHT CONTROL BY THE GERMAN ARMY. THEN IN 1931, A GERMAN TRAITOR, HANS THILO (TEE-LOW) -SCHMIDT,

	SUPPLIED BACKGROUND INFORMATION FOR USING THE ENIGMA MACHINE WHICH AIDED REJEWSKI'S GUESSWORK.
	Stephen Budiansky 01:12:02 The one piece of the puzzle he did not have, was knowing how the keyboard of the Enigma machine was wired to the first rotor. // 01:13:24 Maybe he had a good sense of the lack of imagination of the Germans…..but he thought, well, maybe they wired A to A and B to B and C to C….He tried that and he said the solutions started coming out, as if by magic on this paper in front of him.
	BUT THE GERMANS ROUTINELY CHANGED THE DAILY KEY - THE INDICATOR SETTING THAT DETERMINED THE SCRAMBLING OF THEIR DAILY MESSAGES. THE DAILY KEY WAS DISTRIBUTED IN A MONTHLY CODEBOOK TO BOTH SENDER AND RECEIVER TO CODE AND DECODE MESSAGES. TO FIND THE DAILY KEY, REJEWSKI BUILT AND CONNECTED REPLICAS OF SIX ENIGMA MACHINES TOGETHER THAT RAN THROUGH MORE THAN 17,000 INDICATOR SETTINGS. HE CALLED HIS NEW CONTRAPTION THE BOMBE, BECAUSE OF ITS TICKING NOISE WHILE RUNNING THE PERMUTATIONS.
	David Kahn (53172) 04:10:52 Code making had been mechanized with cipher machines, the Enigma, and now what the Poles were doing after mathemitizing their codebreaking, was carrying it the next step further and mechanizing the mathematized code breaking.
	David Hatch (53162)

	03:16:01 It was a great insight when they invented it. A machine to solve a machine.
	THE POLES SECRETLY READ THE ENIGMA TRAFFIC FOR SEVERAL YEARS UNTIL THEY HIT A HUGE OBSTACLE IN DECEMBER, 1938, WHEN THE GERMANS ADDED TWO NEW ROTORS INTO THE ROTATION. THIS EXPONENTIALLY INCREASED THE NEED FOR MORE BOMBES AND CRYPTANALYSTS TO RUN THROUGH THE DAILY SETTINGS. FEARING A GERMAN INVASION, THE POLES FINALLY CALLED IN THEIR ALLIES, BRITAIN AND FRANCE. IN A SMALL BRICK HUT, IN THE PYRY (PYREE) FOREST SOUTH OF WARSAW, THE POLES REVEALED THEIR ASTOUNDING DISCOVERIES.
	David Kahn 53172 04:13:32 At the proper moment, they stripped away these cloths. They pulled them off, and there in front of the astonished eyes of the British and French codebreakers were replicas of German Enigma machines.
	THE BRITISH WERE ABLE TO SMUGGLE OUT THE MACHINES, TWO WEEKS BEFORE HITLER INVADED POLAND. THEY WENT STRAIGHT TO THE GOVERNMENT'S CODE AND CIPHER SCHOOL, OTHERWISE KNOWN AS BLETCHLEY PARK, AN ORNATE MANSION, 50 MILES NORTH OF LONDON. ALAN TURING, A MATH GENIUS RECRUITED TO BLETCHLEY FROM CAMBRIDGE, SOON MADE A FUNDAMENTAL INSIGHT INTO THE WORKINGS OF THE BOMBES.
	David Hatch (53162) 03:20:54 The original Polish bombe would

	just keep sorting through German military messages until it came upon a key word.
	David Kahn (53172) 04:16:50 Alan Turing realized that there was so many possibilities in the German Enigma machine that they couldn't run through them all, and he had a different approach….he devised a machine which would eliminate most of the possibilities, leaving relatively few to be tested.
	EACH OF TURING'S BOMBES HAD 180 ROTORS THAT CLICKED ROUND LETTER BY LETTER - 20 EVERY SECOND - UNTIL THEY HIT THE CORRECT ONE. BY THIS TIME, BLETCHLEY WAS FILLED WITH HUNDREDS OF CODEBREAKERS WHO WERE DIVIDED INTO HUTS, AND LABORED IN SHIFTS TO SOLVE THE FLOOD OF INCOMING MESSAGES.
	Arthur Levinson- Bletchley Park Codebreaker (53165) 08:20:37 A true meritocracy. And your rank didn't matter a hoot. And if a guy was good, regardless of what rank, he was given a free hand.
	Stephen Budiansky (53143) 02:07:44 It requires a certain almost contradictory combination of talents. On the one hand this ability to deal with detail…but at the same time, this ability to achieve this almost sort of illogical leaps of insight and intuition. It almost is that you wanted Beethoven with the soul of an accountant.
	SOON BRITAIN WAS DECIPHERING LARGE NUMBERS OF THE GERMAN ENIGMA COMMUNICATIONS.
	IN 1943, A BRITISH ENGINEER, TOMMY FLOWERS, CREATED

	'COLOSSUS,' A MECHANISM THAT MOVED CODEBREAKING FROM ELECTROMECHANICAL TO PURELY ELECTRONIC, WHICH WORKED MUCH FASTER. IT READ GERMANY'S MOST COMPLEX CODING SYSTEM - THE 12-ROTOR LORENZ MACHINE USED BY GERMANY'S TOP COMMANDERS INCLUDING HITLER. COLOSSUS WAS A PROTO-COMPUTER CAPABLE OF READING PAPER TAPE AT 5,000 CHARACTERS A SECOND.
	THE ALLIED BREAKING OF THE GERMAN CODES PLAYED A KEY ROLE IN SUCH VICTORIES AS THE BATTLE OF THE ATLANTIC, THE WAR IN NORTH AFRICA AND D-DAY. ALLIED CODEBREAKING SHORTENED THE WAR, SAVED MILLIONS OF LIVES AND HIGHLIGHTED THE POWER OF BRAINS OVER BULLETS. IT ALSO LAUNCHED THE COMPUTER AGE. BUT THERE WAS ANOTHER CODING SYSTEM USED BY THE JAPANESE IN WORLD WAR II, THAT THE AMERICANS WERE JUST AS DETERMINED TO CRACK.
	FACTOID: IN 1952, ALAN TURING WAS PROSECUTED UNDER BRITAIN'S ANTI-HOMOSEXUALITY LAWS. FORCED TO UNDERGO HORMONAL THERAPY, ONE OF CRYPTOLOGY'S GREATEST GENIUSES COMMITTED SUICIDE IN 1954.
	CODES WILL RETURN ON MODERN MARVELS.
ACT FOUR	
	WE NOW RETURN TO CODES ON MODERN MARVELS.
	AT THE CLOSE OF WORLD WAR I, AMERICAN CRYPTOLOGY WAS

	RUDIMENTARY. BUT SINCE THE EARLY 1920s, A LONE GENIUS, WILLIAM FRIEDMAN, HAD BEEN DEVELOPING STATISTICAL METHODS TO SOLVE THE CODES OF THE NEW ROTOR MACHINES WHILE HEADING THE U.S. SIGNAL CORPS. WHEN JAPAN SWITCHED TO A MECHANIZED CODING SYSTEM IN THE MID-1930s, FRIEDMAN'S TEAM OF CODEBREAKERS WAS SOON READING JAPAN'S NEW RED CODE FOR DIPLOMATIC COMMUNICATIONS. BUT SOLVING JAPAN'S CODES WAS A TORTUROUS PROCESS.
	David Kahn (53171) 03:05:41 When you're trying to solve a code, you come in every day and look at inscrutable bunch of letters or numbers…it's anguish….Maybe we should try this. Maybe we should try that. Day after day, month after month, year after year sometimes, until finally, new messages come in which allow you to see some kind of pattern which you hadn't seen before.
	THEN IN FEBRUARY 1939, JAPAN INTRODUCED THE 'PURPLE' MACHINE, A MIND-TWISTING CODING SYSTEM THAT EMPLOYED SEVERAL ROTORS AND TELEPHONE SWITCHES. BUT JAPAN THEN MADE A CRITICAL HUMAN ERROR, AN IMPORTANT FACTOR IN CODEBREAKING THROUGHOUT HISTORY.
	David Hatch (53161) 02:09:04 The Japanese..helped out by sending the same messages in the Red and Purple systems. This allowed Americans to compare the two systems and make some breaks.

	A YOUNG, M-I-T ELECTRICAL ENGINEER IN FRIEDMAN'S GROUP, LEO ROSEN, BUILT A MACHINE TO SIMULATE PURPLE'S COMPLEX SCRAMBLING PATTERNS. BY 1940, THE CONTRAPTION HAD AUTOMATED THE DECIPHERMENT OF THE JAPANESE PURPLE CODE.
	David Hatch (53161) 02:10:39 It was a great intellectual accomplishment….it made the decryption of Japanese messages almost automatic…it sometimes would allow the Americans to read the Japanese ambassador's mail before he did.
	THE PURPLE CODE BREAKTHOUGH LED TO ONE OF THE GREATEST INTELLIGENCE COUPS OF THE WAR. TOKYO'S AMBASSADOR TO BERLIN, HIROSHI OSHIMA MADE A FRONTLINE TOUR OF GERMANY'S DEFENSES IN NORMANDY IN 1943. HE THEN TRANSMITTED A LENGTHY DESCRIPTION BACK TO JAPAN IN THE PURPLE CODE.
	Stephen Budiansky (53144) 03:27:54 He describes in incredible detail, I mean, down to the caliber of the weapons, in the German fortifications, the dimensions of the anti-tank ditches, where mind fields were…I mean, it was really a gold mine.
	THE SOLVED MESSAGE WAS SOON ON GENERAL EISENHOWER'S DESK. HE USED IT TO PLAN THE D-DAY INVASION OF FRANCE, THAT WAS LAUNCHED SIX MONTHS LATER.
	THOUGH PURPLE HAD BEEN CRACKED, AMERICA STILL WORKED DESPERATELY TO SOLVE THE JN-25-B CODE, JAPAN'S SECRET NAVAL

	COMMUNICATIONS. JOSEPH ROCHEFORT, A LONG-TIME CRYPTANALYST FLUENT IN JAPANESE, LED THE EFFORT IN STATION HYPO, THE NAVY'S CODEBREAKING BRANCH IN HAWAII. BY MARCH, 1942, AFTER YEARS OF EXCRUTIATING WORK, JN-25B WAS BROKEN. ON MAY 14, A JAPANESE MESSAGE WAS DECODED OUTLINING A HUGE INVASION FORCE HEADING TO 'AF.' ROCHEFORT AND ADMIRAL CHESTER NIMITZ IMMEDIATELY BELIEVED 'AF' WAS MIDWAY, ONE OF AMERICA'S KEY OUTPOSTS IN THE PACIFIC. BUT WASHINGTON BELIEVED IT WAS THE ALEUTIAN ISLANDS.
	Stephen Budiansky (53145) 04:13:29 It was to shut up the doubters in Washington that Rochefort carried out what's now this famous stunt of having a message sent to Midway, ordering them to send a message announcing that their desalination plant had broken…then a few days later a JN-25 message was broken in which the Japanese said that they had intercepted this American message saying that AF was short of water…this really dotted the I and crossed the T.
	THE INVASION OF MIDWAY WAS THE GRAND PLAN OF ISOROKU YAMAMOTO, JAPAN'S LEGENDARY NAVAL COMMANDER. THE INTENT WAS TO TAKE OVER THE ISLAND, DRAW OUT THE REMAINING AMERICAN FLEET FROM PEARL HARBOR AND DESTROY IT WITH A SURPRISE ATTACK. ON JUNE 4, 1942, THE JAPANESE BEGAN TO ATTACK MIDWAY, BUT LURKING ON THE HORIZON WERE THE COILED FORCES OF THE U.S. NAVY.

	Stephen Budiansky (53145) 04:11:51 Knowing in advance what the Japanese plans were allowed Nimitz to get his carriers there first and essentially surprise the Japanese.
	David Kahn (53171) 03:14:26 We knew where the Japanese fleet was coming. We were able to hover off their flank and unsuspecting of the Japanese, hurl ourselves on the Japanese, sink four carriers, and send the Japanese battleships and carriers reeling back to Japan.
	Stephen Budiansky (53145) 04:11:51 That knowledge not only was the turning point for the Battle of Midway, but the Battle of Midway was the turning point in the entire Pacific War.
	IT WAS A STUNNING AND FLAWLESS OPERATION. AND IN ANOTHER PART OF THE PACIFIC THE AMERICANS WERE LAUNCHING ONE OF THEIR OWN CODES - ONE THAT WOULD NEVER BE BROKEN IN WORLD WAR II. PHILIP JOHNSTON, A RETIRED ENGINEER LIVING IN LOS ANGELES, PROPOSED USING THE NAVAJO LANGUAGE TO THE MARINES IN 1942. JOHNSTON GREW UP ON A NAVAJO RESERVATION AND WAS FLUENT IN IT'S COMPLEX FORMS OF CONJUGATION, SOUNDS AND STRUCTURE. IT WAS REMOTE - ONLY ABOUT 30 WHITE AMERICANS COULD SPEAK IT. NO GERMAN, JAPANESE OR ITALIAN HAD EVER STUDIED IT. THE NAVAJO WERE ALSO ONE OF AMERICA'S LARGEST TRIBES WITH A POTENTIALLY HUGE POOL OF CODETALKERS.
	Dr. Sam Billison - Navajo Codetalker

	(53099) 09:12:04 We use what we call a phonetic alphabet, so we use it by sound // 09:13:59 it's a nasal sounds and guttural sounds and interchangeable.
	WITHIN WEEKS OF HEARING JOHNSTON'S IDEA, THE MARINES WERE TRAINING 29 NAVAJO CODETALKERS NEAR SAN DIEGO.
	TO AVOID CONFUSION, MANY NAVAHO WORDS FROM THE NATURAL WORLD WERE USED TO INDICATE SPECIFIC MILITARY TERMS.
	Dr. Sam Billison (53099) 09:15:06 Chetavaji in Navaho is turtle. And when you send a message and chetavaji on the radio, the receiver writes down tanks, T-A-N-K-S.
	BY AUGUST, 1942, THE FIRST GROUP OF NAVAJO CODETALKERS SAW ACTION DURING THE INVASION OF GUADALCANAL. BY THE END OF THE YEAR AN ADDITIONAL 83 CODETALKERS WERE SERVING IN ALL SIX MARINE CORPS DIVISIONS.
	David Kahn (53171) 03:30:18 If you wanted to communicate a written message securely, you had to type it out or write it out. You had to give it to a code guy…this could take an hour or several hours. With the Navajo code guys, it was instantaneous.
	THE NAVAJO SPOKE DIRECTLY OVER THE RADIO, SENDING AND RECEIVING BATTLEFIELD COMMUNICATIONS FROM BOTH FIELD HEADQUARTERS AND FROM THE FRONT LINES IN THEIR NATIVE LANGUAGE.

	Dr. Sam Billison (53099) 09:35:31 When you send a Navajo code…the receiver gets it….gives it to the commanding officer. That's how fast it was, two minutes against two hours.
	IN THE ATTACK ON IWO JIMA, THE NAVAJO CODETALKERS SENT MORE THAN 800 TOP SECRET BATTLEFIELD COMMUNICATIONS, ALL WITHOUT ERROR.
	BY WAR'S END, THERE WERE 420 NAVAJO CODETALKERS. AFTER THE WAR, THE U.S. GOVERNMENT FORBADE THEM TO TALK OF THEIR UNIQUE CONTRIBUTIONS BECAUSE OF THE SECRECY OF THEIR CODE. ONLY IN 1968 WAS THE NAVAJO CODE MADE PUBLIC AND IN 1982, THE CODETALKERS WERE FINALLY HONORED WITH A SPECIAL COMMEMORATION DAY.
	David Kahn (53171) 03:29:30 America owes the Navaho codetalkers the lives of many of its sons.
	THE GREATEST TRIBUTE WAS THAT THEIR CODE WAS NEVER BROKEN. BUT FOR CODEMAKERS, THE HUNT FOR A TRULY UNBREAKABLE CODE IS AN OBSESSION THAT CONTINUES INTO THE AGE OF COMPUTERS.
	FACTOID: AMERICAN CODEBREAKER WILLIAM FRIEDMAN INVENTED SEVERAL CRYPTOLOGIC MACHINES, TWO OF WHICH WERE SO SECRET, PATENTS WERE NEVER FILED.
	CODES WILL RETURN ON MODERN MARVELS
ACT FIVE	
	WE NOW RETURN TO CODES ON

	MODERN MARVELS.
	FOR CENTURIES GOVERNMENTS HAD CONTROLLED CRYPTOLOGY. THAT WOULD CHANGE WITH THE MODERN AGE. SOON AFTER WORLD WAR II, COMPUTERS BEGAN TO CREATE CODES OF ALMOST INFINITE COMPLEXITY.
	David Kahn (53173) 05:09:55 There's a rule of thumb in cryptography. If you double the number of combinations that the code makes, you have to square the number of combinations that the codebreaker has to try. So one guy is going from five to ten. But the codebreaker has to go from five to 25…it's much easier to make the number of combinations virtually impossible to test.
	BUT THIS NEW ENCRYPTION WAS STILL ONLY ACCESSIBLE TO THE GOVERNMENT. IN 1952, PRESIDENT HARRY TRUMAN FOUNDED THE NATIONAL SECURITY AGENCY, THE GREATEST COLLECTION OF COMPUTER AND CRYPTOLOGIC TALENT IN THE WORLD. ITS CHARGE WAS TO INTERCEPT AND DECRYPT INTELLIGENCE FROM ALL OVER THE GLOBE.
	BY THE 1970s, MORE BUSINESSES BEGAN USING COMPUTERS TO ENCRYPT COMMUNICATIONS. BUT DISTRIBUTING SECRET KEYS - NEEDED TO ENCODE AND DECODE MESSAGES – REMAINED CRYPTOLOGY'S GREATEST HISTORICAL PROBLEM. BUSINESSES HAD TO PHYSICALLY FLY COURIERS TO DOZENS OF DISTANT OFFICES TO DELIVER THE SECRET KEYS TO AVOID INTERCEPTION AND ENSURE ABSOLUTE SECURITY.
	BUT KEY DISTRIBUTION WAS NOT

	CRYPTOLOGY'S ONLY PROBLEM. BY THE 1970s, SOME PEOPLE WERE CONCERNED ABOUT THE GROWING CODEBREAKING POWER OF THE GOVERNMENT BECAUSE OF COMPUTER TECHNOLOGY.
	Phil Zimmermann, Inventor - "Pretty Good Privacy" Software (53084) 01:25:01 I think the biggest threat to privacy is Moore's Law….It's the power of computing doubling every 18 months. The human population is not doubling every 18 months. But the ability for computers to keep track of us is. Surveillance technology with computers behind them to analyze the surveillance data, can give rise to an omniscient government…and it's not clear that democracy can survive omniscience.
ANIMATION	BY THE MID-1970s, A TRIO OF STANFORD CRYTOGRAPHERS, WHITFIELD DIFFIE, MARTIN HELLMAN AND RALPH MERCKLE, CREATED A THEORETICAL MODEL FOR CODED COMPUTER COMMUNICATIONS THAT ELIMINATED THE NEED FOR A SECRET DISTRIBUTION OF KEYS. IT ALSO SOUGHT TO OFFER POWERFUL DIGITAL ENCRYPTION TO A PERCEIVED FUTURE OF MASS COMPUTER USERS AS A COUNTERWEIGHT TO GOVERNMENT SPYING. CALLED PUBLIC KEY CRYPTOGRAPHY, IT GAVE EACH COMPUTER USER A PAIR OF DIFFERENT BUT RELATED KEYS, ONE PUBLIC AND ONE PRIVATE. NOW SAY BOB WANTS TO SEND A SECRET MESSAGE TO ALICE. BOB WOULD USE ALICE'S PUBLIC KEY FOR ENCODING. BUT ONLY ALICE COULD USE HER PRIVATE KEY TO DECODE THE MESSAGE. NO PHYSICAL TRANSPORTATION OF

	SECRET KEYS. AND NOW EVEN BOB AND ALICE COULD THEORETICALLY HAVE ACCESS TO ENCRYPTED COMMUNICATIONS HIDDEN FROM THE MOST POWERFUL INVESTIGATIVE FORCES IN GOVERNMENT. COMPLETE PRIVACY.
	David Kahn (53173) 05:16:11 None of the other developments in cryptography that I have seen, from the beginning of codes and ciphers themselves // has had the impact or has been an original a concept in cryptography as Whitfield Diffie's invention of public key cryptography.
	WITHIN A YEAR, THREE M.I.T. RESEARCHERS, RONALD RIVEST, ADI SHAMIR AND LEONARD ADLEMAN CREATED A SERIES OF MATHEMATICAL EQUATIONS USING PRIME NUMBERS THAT MADE DIFFIE'S THEORY PRACTICAL.
Public Key Animation	AS A SIDE NOTE, A GROUP OF THREE SCIENTISTS, JAMES ELLIS, MALCOM WILLIAMSON AND CLIFFORD COCKS, WORKING FOR BRITAIN'S GOVERNMENT COMMUNICATIONS HEADQUARTERS, APPARENTLY INDEPENDENTLY INVENTED PUBLIC KEY CRYPTOGRAPHY BY THE MID-1970s, JUST BEFORE WHITFIELD DIFFIE. THEIR WORK WAS CLASSIFIED AND IT WASN'T UNTIL 1997 THAT PUBLIC ACKNOWLEDGEMENT OF THEIR FEAT WAS RECOGNIZED.
	AS FOR THE THREE M-I-T INVENTORS, THEY FORMED RSA DATA SECURITY IN 1982, THE FIRST COMPANY TO COMMERCIALIZE PUBLIC KEY CRYPTOGRAPHY AND LAUNCH SECURE E-COMMERCE.

	Len Adleman - Co-inventor, RSA Crypto Cipher (53185) 05:21:15 The market we were going after in 1982, was the Internet market, okay. But we were so premature because it was to be 15 years later, that the World Wide Web took off.
	BUT THE NATIONAL SECURITY AGENCY DID NOTICE AND DESPERATELY TRIED TO STOP THE SPREAD OF PUBLIC-CRYPTOGRAPHY. IN 1986 THE GOVERNMENT STOPPED LOTUS DEVELOPMENT FROM EXPORTING ITS SOFTWARE BECAUSE IT INCLUDED RSA ENCRYPTION. THEN IN 1993, THE GOVERNMENT INVESTIGATED PHIL ZIMMERMANN FOR CREATING AND DISTRIBUTING PRETTY GOOD PRIVACY - A SOFTWARE THAT USED RSA ENCRYPTION, OVER THE INTERNET. P-G-P, COULD BE USED ON ANYBODY'S PERSONAL COMPUTER INSTEAD OF JUST THE GIANT MACHINES USED BY THE GOVERNMENT AND BUSINESSES.
	Phil Zimmermann (53084) 01:11:04 There was a time when NSA held a monopoly on this kind of technology. But over the past 20 years, that monopoly has eroded, and now academic cryptography has reached parity with the NSA…And PGP uses the best of the cryptographic algorithms and has made it available to the masses.
	THE NATIONAL SECURITY AGENCY WAS TERRIFIED THAT CRIMINALS WERE NOW ACCESSING THE WORLD'S MOST POWERFUL UNBREAKABLE ENCRYPTION. THE N-S-A BELIEVED P-G-P WAS SEVERELY COMPROMISING ITS

	CODEBREAKING AND INTELLIGENCE-GATHERING ABILITIES.
	Phil Zimmermann (53084) 01:18:13 Many times I've been worried about if criminals and terrorists were to use this technology. And I did a lot of soul searching on it. I sometimes lost sleep thinking about it. But …individual governments, like Stalin and Hitler, have killed more people than all of the criminals of the 20th century combined, all over the world.
	BY 1994, RSA ENCRYPTION WAS WIDELY USED IN MOST U.S. SOFTWARE AND COMPANIES WERE PUSHING TO EXPORT IT. THE GOVERNMENT URGENTLY SOUGHT A COMPROMISE BY INTRODUCING THE "CLIPPER CHIP," A GOVERNMENT CHIP THAT WOULD BE INSTALLED IN COMMUNICATIONS DEVICES. THE CHIP, LIKE A WIRETAP, COULD ONLY BE ACCESSED BY THE GOVERNMENT THROUGH A COURT ORDER. LAW ENFORCEMENT COULD STILL EAVESDROP ON SUSPECTED CRIMINALS BUT GRANT THE PUBLIC A LEVEL OF PRIVACY.
	Dorothy Denning - Professor of Computer Science, Georgetown University (53147) 06:14:15 People were concerned that it was voluntary to start out with but that it would become mandatory, that it would be pushed upon them. They were concerned about loss of personal privacy.
	Len Adleman (53185) 05:35:02 Do you want to control your private communication just by yourself, or do you want to be partners with the Government in controlling your private

	communications? Ultimately the society has decided that we want to keep privacy to ourselves.
	AFTER A FIVE-YEAR FIGHT, AND A HUGE PUBLIC BACKLASH TO THE PROPOSAL, THE CLINTON ADMINISTRATION GRANTED BUSINESSES THE RIGHT TO EXPORT PUBLIC CRYPTOGRAPHY. BY 1996, AFTER M-I-T HAD PUBLISHED P-G-P IN A BOOK AND POSTED IT ON ITS WEBSITE, THE GOVERNMENT BACKED OFF ITS INVESTIGATION OF ZIMMERMANN.
	David Kahn (53174) 06:02:09 Even though government has intruded increasingly into private lives and has greater capacities these days to intercept communications, the growth of encryption has made it possible for individuals to protect themselves and protect their privacy in a way that had never been able to be done before.
	Len Adleman (53185) 05:48:36 Historically there's been a battle between cryptographers who make the codes and cryptanalysts who break the codes. Edgar Allen Poe once said ….that any code a man can invent, another man can break ….But it turns out that that's probably incorrect. The best mathematical evidence is that that's not the case, that in fact codemakers do win over codebreakers.
	David Kahn (53173) 05:26:34 Codebreaking will last as long as people make mistakes…But the code systems themselves are getting better and better. They can't be broken now if properly used….So I think we're in an era of the slow death of the codebreaker much as I regret it in a way, and increasingly in the era of the codemaker.

	BUT THROUGHOUT HISTORY, NEW CODES HAVE ALWAYS BEEN DECLARED UNBREAKABLE, ONLY TO BE EVENTUALLY BROKEN. AS CODES ENTER THE REALM OF QUANTUM COMPUTERS, HUMAN INGENUITY WILL BE TESTED ONCE AGAIN. ONLY TIME WILL TELL THE VICTORS.
	END