Cryptography and the origins of spread spectrum

Engineers during World War II developed an unbreakable scrambler to guarantee secure communications between Allied leaders; actress Hedy Lamarr played a role in the technology.

Deep in the guarded labyrinth of the newly constructed Pentagons, an army lieutenant with top security clearance inserts a voltmeter probe into a horseshoe-shaped, 7-foot-panel of electronic equipment. The apparatus is top secret; the room where it sits, with its polished tile floor, is windowless.

Tip to tip with the horseshoe stands a duplicate horseshoe. Each is dominated by a railroad clock graduated in 24-hour time and set to Greenwich mean time. Within each horseshoe, ovens hold quartz crystals vibrating at an extremely precise frequency. Near each horseshoe's tips stand two photographs with some of the most accurate turntables ever made. But they reproduce sounds quite different from such popular songs of the day as "Marry the Man I Love." It was the summer of 1944. World War II was at its climax. In Normandy, the Allied armies had begun to press the line out of Hitler's Third Reich. But the conflict was not over, and the Allied leaders still had to make plans and resolve disputes about tactics and supplies.

Lieutenant Gordon A. Smith, 24, who had recently graduated as an electrical engineer from the Virginia Military Institute, was making routine checks on a new transmitting radiotelephone scrambler system in the Pentagon in Washington, D.C., that permitted the Allies a secure policy in perfect security for the first time in radiotelephone history. The system pushed technology to its limits, maintaining, for example, synchronization of certain elements to a degree that then unprecedented in communications. And it pushed technology beyond its former limits, creating, as it did so, some of the practical foundations for techniques as broadly useful today as pulse-code modulation and spread-spectrum transmissions.

Suddenly a member of the scrambler unit emerged from one of the side rooms and said, "Okay, let's set sail on the air. We have a call for London from the White House." Smith put down his probe and moved to an oscilloscope on one of the horseshoes. He picked up a telephone. One of the sergeants radioed the scrambler system's London terminal—at Oxford and Duke Streets in the stonework of the annex to Selfridge's department store—with its horseshoe identical to those in the Pentagon. He told the personnel there to begin the operating procedure and to notify Prime Minister Winston Churchill that a call was coming for him.

Secret telephone in the Cabinet War Rooms

Churchill took and made calls from a dot-matrix line in the Cabinet War Rooms, a vast bombproof warren of offices and domed basements dug between two streets—Whitehall and the Home Guards Parade—and covered with a thick reinforced concrete slab. To that room an extension had been run inside a steel pipe. Smith's telephone was a new invention which could be used in a secure telephone system.

Cryptography

Cryptography is the science of writing secret messages. Ciphers are codes used to transform messages into secret code. The first unbreakable scrambler

The call lasted from 3 to 7 minutes. All went well. But after the President and the Prime Minister hung up, Smith was left with a peculiar feeling: he had been a witness to history—but he could not tell anybody about it.

In 1941, the telephone had a special high-quality, pressure-sensitive dynamic microphone (input) that responded to frequencies below 200 hertz, important for low-pitched male voices such as Churchill's. A London and Washington time chart (1), an earphone for a secretary (2) and operating instructions (3) were included in the telephone facility.

2

Figure 1-1. High-speed telephone at the British Cabinet War Rooms underwrote the Government Buildings in Whitehall, London, was used by British Prime Minister Winston Churchill during the Second World War to talk with U.S. President Franklin D. Roosevelt. Designed and built by Bell Labs and purchased for the Government Departments in Manhattan in 1941, the telephone had a special high-quality, pressure-sensitive dynamic microphone (input) that responded to frequencies below 200 hertz, important for low-pitched male voices such as Churchill's. A London and Washington chart (1), an earphone for a secretary (2) and operating instructions (3) were included in the telephone facility.

of some presidential aide but the familiar aristocratic accents of Franklin D. Roosevelt. "Is it you, Willie?" Roosevelt asked. And then Smith heard Winston Churchill's voice, somewhat mechanical but instantly recognizable in response. The two conversed, Roosevelt saying that people in America were getting anxious for more military action, and Churchill replying that he needed more ships. But Smith, after his initial surprise, paid little attention to the conversation. He was concentrating on keeping green dots on the oscilloscope line up to the diagonal so that the voltages of the noise-masked communications signals were increasing in the proper steps. And, though he was not nervous about handling such a high-level communication, he did keep hoping that everything would work.

were increasing in the proper steps. And, though he was not nervous about handling such a high-level communication, he did keep hoping that everything would work.
A Soviet SIGALY?

Roosevelt and Churchill were not the only world leaders of their day to take an interest in securing their telephone communications. Though Adolf Hitler seems not to have used a scrambler, it is probably better known. When telephone, his conversations going by land line, Josef Stalin had the presidents of the Soviet Union unit to develop a secret telephone apparatus for him to use.

Scientists from the Soviet Union and Eastern European countries were working on a similar system called MARINGO, on the outskirts of Moscow. Some of the scientists involved in the project were arrested in a guided tour of the Soviet Union. The creators of SIGALY, they based their work on the vocoder, while they learned about it from American engineers. This may well have been the vocoder developed by Hershfield and his colleagues. Vol. 18, December 1938, pp. 122-23.

The vocoder was said to have been the first practical application of a guided tour of the Soviet Union. The creators of SIGALY, they based their work on the vocoder, while they learned about it from American engineers. This may well have been the vocoder developed by Hershfield and his colleagues. Vol. 18, December 1938, pp. 122-23.

The vocoder was said to have been the first practical application of a "slow" signal, whose effect was to make the voice sound "slow" or "slow." This was a significant improvement over traditional vocoders, which used simple modulation schemes to achieve the same effect.

Vocoder speech synthesizer studied

In their studies in the early 1940s, the Bell Labs teams working on speech synthesis had looked into the possibility of using the vocoder, a speech analyzer and synthesizer developed by Bell Labs a few years earlier to investigate reducing the bandwidth needed to transmit speech.

The vocoder analyzer first filtered the speech frequency spectrum in 30 equal bands of 500 Hz each. Subsequent rec

The Bell Laboratories were the first to use a device for telephone transmission, containing signals up to 25 Hz. A signal corresponding to the pitch, or fundamental vocoder frequency, controlled the wave shape, which was also defined. The information in these 11 separate channels, which together occupied a substantially smaller frequency band than the normal voice spectrum, was transmitted to a receiver. In the synthesizer, the fundamental frequency was generated from the pitch signal, or, alternatively, a broadband noise generator was activated to produce unvoiced, hissing sounds such as "taas." The pitch or noise signals were applied to filter identical to those in the transmitter. The signal produced by each filter was subsequently amplitude-modulated by its corresponding low-frequency signal and the 11 channels were combined to reconstruct the speech, an in apparent to mimic the dynamic acoustic resonances of the human mouth, tongue, nose, and throat.

But the results sounded very artificial, as Bell Labs teams did little with the vocoder. Then, early in 1941, the British Post Office wrote for information about it, hinting that it was to be served in a scrambler system, whereupon (the Bell Labs people put the vocoder and the masking principle together to create their own scrambler.

In doing so, however, they faced with the problem of how to apply the one key that ensures perfect secrecy in any cryptographic system. This key is a sequence of symbols—such as zeros and ones—that is perfectly random and never repeated. These two characteristics of the key provide the cryptanalyst with the information needed to reconstruct and so they determine the "plaintext"—the message to be intelligible. Even given a portion of the key, the cryptanalyst cannot predict the next symbol and so cannot even begin to solve the next message. Nor will trial and error work, because it would merely generate all messages of the length of the cryptogram with no indication—because the key is random—as to which message is right. This so-called one-way key device was devised by a Signal Corps major, Joseph O. Mauzberg, and embodied in a device for teletypewriters that automatically added the electrical pulses of the key to the pulses of the plaintext to produce the ciphertext. This device was well known to Bell engineers, for it had been created in December 1917 by one of its predecessors, an American Telephone and Telegraph engineer named Gilbert S. Vernam. The Vernam system added in binary. But how could keys consist of a series of ones or of zeros? As a plaintext, as in the vocoder? The leader of the labs' speech-privacy teams, Ralph K. Potter, who held a couple of top-secret passes, suggested that the individual vocoder amplitude channels could be treated as on-off channels. But the speech was badly mutilated. Each channel was then divided into two to reestablish the spectral measurement of the speech. This helped, but it was apparent that more amplitude levels would be needed to provide acceptable quality. In the end, 10 voice-amplitude spectrum channels were used plus two channels, for sending the pitch—or "buzz"—and the "his" signals. Each of the 10 spectrum channels was sampled 50 times per second—once every 20 milliseconds. At each sampling time, the 10 amplitude samples were each quantized to one of six levels on a logarithmic scale 16 decibels apart, resulting in 1024 digit. Samples of the pitch-frequency measurement were quantized to a four scale of 56 levels, represented by a pair of binary digits. Each 20 milliseconds, then, 12 binary digits were generated and transmitted to the receiver. The sampling of an analog signal with its quantization and coding is today known as pulse-code modulation, and SIGALY marked its first use for speech transmission.

Enter the X-system

Multiple levels in the vocoder channels required multiple levels in the key. But it was not immediately clear how adding more levels should be done, say 4, to a binary key. A way might be to within the binary bound—of 6 of the vocoder channel. In a dis
The intelligibility was good and improved as the listener gained experience. And though some users found the voice quality unsatisfactory, most were willing to accept some distortion for absolute security in a telephone call.

To produce a key that had the required randomness, the engineers used mercury-vapor rectifier tubes to generate wideband thermal noise, which was perfectly random. The output of these 14-in.-high, 4-inch-diameter tubes, which emitted a bluish light, was sampled every 20 milliseconds and the samples were quantized nonuniformly into six levels of equal probabilities. These were recorded on vinyl disks that resembled the transcriptions that radio stations then used for music and radio programs—low-noise disks that were larger and revolved more slowly than the then-standard 78-rpm records sold to the public. These masters, made by Bell Telephone Laboratories at the Graybar Varick Building at 140 Varick St. in lower Manhattan, were taken under guard to the World Broadcasting System at 711 Fifth Ave., where two pressing machines were made. The masters were destroyed and the pressings (codenamed, rather transparently, SIGRURS) taken to the army's code-making and code-breaking agency at Arlington Hall, a former girls' school in Arlington, Va., for distribution by courier to the sending and receiving stations.

Synchronization of the records at both ends was made practicable in part by the relatively long sampling interval of 20 milliseconds, in part by the availability of a sufficiently accurate frequency standard. This was provided by a highly stable 100-kilocycle quartz crystal oscillator that was kept in an oven in the Sigsalohouse to maintain its precision of one part in 10

In another Bell Telephone Laboratory's secret telephone patent filed for and awarded on the same dates as Potter's page 74, Inventor Robert C. Mathis portrays yet another speech-encryption scheme. In its transmitter here the pitch (CH) and spectrum-defining signals are quantized by stepping circuits (31) into typically five levels. A record produces a random million—more than sufficient to keep within the plus or minus 1 millisecond required, with only very infrequent manual adjustments.

Telephones protected against tapping

As early as 1943 in Room L30, formerly the sound movie laboratory, Blye felt that its secrecy was perfect: "We were convinced that we could have dropped a terminal in Berlin and without the records no one could figure it out." Turing finally approved the system, and, on his recommendations, the British declared themselves "completely satisfied as to its security for voice communications. They were not pleased with the fact that--as Turing put it--"if the equipment is to be operated solely by U.S. personnel it will be impossible to prevent them listening in if they so desire." But the British chiefs of staff concluded that "we could not do anything but agree."

Throughout the war, Blye's group manufactured a dozen terminals. Those were installed successively in Washington; London; Algiers; Brisbane, Australia; Fort Shafter, Hawaii; Washington again (primarily for the Pacific); Oakland, Calif.; Paris after its liberation; and, on a 25-ton lighter in the Pacific; after a trip to Germany's surrender; and Berlin. All could interconnect, and test connections were sometimes made from London through Washington to Australia: they worked perfectly. Several terminals had conference facilitators, so that several persons around a table could hear, and simultaneously hear the person on the other end of the call, though the telephone had to be handed to anyone who wanted to speak.

Training conducted in secret

The Signal Corps ran Sigsalohouse, and so personnel for it came from the Army. Despite that organization's reputation for nu...
Spreading the spectrum

SIGSALY's employment of more radio bandwidth than was nec-

essary for the information it carried was a method of trans-

mission that is fundamentally different from the standard kind

and that has only recently been gaining widespread recogni-

tion and use. This is spread spectrum.

Ordinary forms of radio signals employ a relatively narrow

band of frequencies through the modulation of a single-fre-

quency carrier signal. Their success in delivering their message

depends on the quality of the signal, the frequency stabili-

ty. But they suffer from certain disadvantages. Noise in the

transmitter or interference at the receiver may distort the signal

thus vulnerable to jamming. The ease of signal detection can

aid unintended eavesdroppers in discovering the signal's exis-

ence, in finding the direction toward its source, and in inter-

cepting its messages—at sources of military intelligence. And

in a crowded electromagnetic spectrum, each signal must com-

pete with those emanating from other transmitters.

But the laws of nature do not dictate that ordinary, frequency-

limited radio transmission be the only kind. This kind originated

first in a number of wireless experiments in the early 1920s. Later

in the 1920s, the idea of a different kind of transmission

indication was carried over into parts of the world. In one embodiment of this idea the radio carrier is controlled by a

sequence of numbers or a baseband signal. This

reversal, which knows this sequence, uses it to reconstruct the

original signal.

One way of doing this is called frequency hopping. The trans-

mitter actually carries successively on a different set of

frequencies in rapid short blocks in a controlled order over a wide

range. The receiver knows this order, picks up the2 baseband blocks, and assembles them into the original message.

In time-hopping—a similar technique in the time domain—the

transmitter encodes its information-carrying signal during a

fraction of a time interval, and where it does vary from one instance to another, it results in a variation controlled by the

pseudo-random sequence. The receiver, having the sequence,

knows when the signal is on and off; it receives the information.

The third major form of this kind of transmission is called

direct-sequence spread spectrum. In this case, it utilizes

pulses so much shorter than the bits of the message that they

are called "chips." These chips successively multiply, of the

in the time domain, the transmitter's signal. At the receiver, the

coming signal is multiplied by the chip sequence to recover the

original signal.

Because this transmission idea, in all its forms, utilizes a far

wider bandwidth per unit of information than does the

bandwidth required by the original information signal, it has
come to be known as spread spectrum transmission. The word was devised in the 1950s by Madison Nicholson and John Raney, two

engineers with Bell Labs and the Electronic System

Division in Buffalo, N.Y., who pioneered in developing the system.

The system enjoys a number of advantages over ordinary

radio transmission. The two chief ones attract the military, its

relatively immune to jamming and eavesdropping transmissions, and its

comparative insusceptibility to jamming. The latter stems from its wide bandwidth, no matter how strong, on a single frequency, or even on bands of frequencies, will block out only a very small portion of the total spectrum used

to transmit the information. Its relative indestructibility, at least in its direct-sequence form, derives from two facts: an ordinary narrow-band radio would miss nearly all of the transmission, and it would hear the transmission not as signal but as noise. Even if it monitoring receiver were wideband, the signal is so spread that it lies below the level of thermal noise of American firms and universities.

At the Massachusetts Institute of Technology in Cambridge,

Yu King Liu, Jerome Weisner (later a presidential assistant,

and Thomas E. Madsen collectively developed in 1947

the first high-performance electronic correlators. At about the

same time, engineers at the Bell Telephone Laboratories of

Sylvania utilized spread spectrum for a missile guidance and

navigation system. Norbert Rieger, an engineer at the Federal

Telecommunication Laboratories in Nutley, N.J., a subsidiary of

the International Telephone and Telegraph Co., used the

Manchester telephone digital-data transmission system in a pseudorandom

generator. Meanwhile, early in the 1950s, fundamental research in

spreadingoperations was beginning at the Lincoln Laboratory of

M.I.T. under Robert Fano and William Davenport.

In 1951 Lincoln Laboratory was developing a spread-

spectrum radio equipment for the Signal Corps, using digital

pseudorandomizing and synchronizing techniques worked out by

camperman's student, Paul E. Green. First trials of this

long-range, fixed transmitting, fixed receiving, called the Fkco,

began in August 1954 between Davis, Calif., and Deal, N.J. By

the spring of 1955 it was overcoming jamming. The end of the

year, the U.S. Army Signal Corps let a production contract to

Sylvania Electronic Defense Laboratory in Mountain View,

Calif., and, in January 1959, an installation near Washington,

D.C., became the first in a network with posts in Germany,

Japan, and the Philippines. The FSC served a number of years

under other systems replaced it.

The value of spread spectrum was emphasized in the sum-

mer of 1952 when Israeli aircraft and downed Syrian MIGs in

the Bekaa Valley with a loss of only two Israeli aircraft. This

confirmed the value of spread spectrum. It allowed Yom Kippur War, when Israeli planes, lacking spread spectrum, appeared to have been jammed. Last February, Military Elec-

tronics/Cointermeasurics magazine gave one reason for the

unheard-of 50.1 kilo ratio of 1962: "The positioning of the Israel F-16s and P-30s would not have been possible without secu-

rity and digital communications. Syrian jammers were unable to degrade the communications of the opposing force sig-

ificantly because, it went on, of frequency-hopping radios

manufactured by Israel's Taelon Electronics Industries Ltd.

The advantages of spread spectrum have led to its use in

communications by such high-risk programs as the Strategic

nuclear, in the MILSTAR communications satellite, in the Global

Positioning System for navigation, in radar astronomy, and in

telephone, but Roosevelt insisted that a study be made as to the

best method of improving communications between Washington

and London. The two government officials considered how

to know Churchill's habits better. Roosevelt seemed less than delighted to be troubled at all hours of the day and night by the Prime

Minister, whose later breakfasts and conferences for calling where the mood struck him were compounded by the six-hour time differ-

ence between London and Washington. So the first terminal was

installed not in the White House but in the Pentagon in March

1943. The second went in May to London. The first overseas test

call was completed on June 29, opening ceremonies with a formal
call to London took place July 15. Shortly afterward, the OPEPs, or extension, to the under-ground Cabinet War Rooms was installed in Churchill’s tiny office.

But as of October, the four calls that had been placed through it all still been, in the British memorandum’s under-stated term, "inoperative," and the likelihood that Churchill had continued to call Roosevelt from the Cabinet War Rooms using the A-3 scanner instead of going to the SIGSALY in St. Elmo’s nest, merely why the British Churchill was continuing to interrupt his calls. It overheated him talking with Roosevelt on the OPEPs and was suggested to the Germans that the two had been dealing with the new non-Munsoni government in Italy and that hardened Germany’s decision to get rooms into Italy and the Soviet Union.

For Churchill, a cigar and identity

In April 1944, by Lieutenant Stephen M. Gels of the London detachment. Before Gels went to the Cabinet War Rooms, he bought the biggest cigar he could find—at 10 cents—a present to the prime minister. When Churchill arrived, wearing white dress, he complained that the system delivered excellent intelligibility but not necessarily the personalities of its speakers.

If synchronization failed, he said, Churchill would hear a sound that resembled the hiss of a needle on a phonograph. If this happened to the British radio, the Germans would be out of tune, only needed to be retuned to restore the message to its original condition, as Churchill’s accomplishment, said, "Oh, you may stay here if you wish." Gels replied, "I do not think it good that I do so, Mr. Churchill." The prime minister acceded. Gels made the call, which lasted about 89 minutes. The last and sent Gels an autographed copy of his book My Early Life.

The third terminal was installed in October 1943 with considerable difficulty in the St. George Hotel in Algiers, where’s banqueting hall was 11 irregularly shaped rooms with different floor levels and varied ceiling constructions. The air-conditioning ducts, prototypes for 14-ft. walls, would not fit the hotel’s walls, which were from 24 to 38 in. thick and merely piles of rocks with sand between them, plastered on both sides. "An attempt to make holes in the solid rock or in soft sand which runs out the hole." Another problem was that SIGSALY took up much more room in the hotel’s banqueting hall than in the St. George’s dining room. It’s "giving out air circulation to his wine cellar, causing his champagne to spoil."

Not everyone enjoyed this new technology of the telephone, however, even though SIGSALY secured it. General Douglas MacAr-thur, commander of the Southwest Pacific Theater, refused to talk over SIGSALY because he was not convinced that it was fully secure; he, as Colonel Curtis LeMay, chief of staff for the Pacific Air Force, preferred the teleprinter system known as SIGTAC that embalmed MacArthur’s one-time system in the on-line form invented by Venetians, while SIGSALY relied on radio, distrusting its security and complaining that he often could not understand what he heard over the radio.

No every SIGSALY connection was perfect. A SIGSALY operator noted that a conference from Algiers in February 1944 was "poor." In a connection with London, "some British voices did not sound out our picture circuits," delays occurred. One offi-cial heard a call only 9 minutes 50 seconds after midnight to 6:45 a.m. Some times circuits were noisy.

But in general, officers and officials liked SIGSALY. And SIGSALY was one of the prime secrets of the war: once the greatest secret of the war: the atomic bomb. The supersecret transatlantic which relayed the message of the delivery of the two existing weapons to Stalin, whom they were flown to Hiroshima and Nagasaki.

SIGSALY was extensively heavier in the European theater. In its first year of operation, 448 conferences were conducted over the London terminal. Most did with the ninety-defense difficulties of war.

General strategy by telephone

Sometimes, however, SIGSALY served aspects of grand strategy.

One instance involved Yugoslavia and whether Britain should support the independent prince, Draya Mihailovic, or the suc- cessful Communist, Marshall Tito, in the partisans’ resistance against Germany. Into that occupied Balkan nation Churchill had assigned a duty to a brigade. Field Marshal Freyza Maclean. After dealings there, Maclean and the others by air, and in April 1944 he returned to Algiers to report to the prime minister. A cable came back from Churchill, "Call Tito or a type of SIGSALY he chose SIGSALY. At about 2 p.m. on April 17, Maclean, in full Yugoslav uniform, appeared at what he described as "the brightly lit cabinet room in the second floor," where "a startlingly pretty WAC sergeant" was ready to record on a Dictaphone with a new tape which had been linked to London was with Wash-ington, and he wasEstablishing was the Chief of TS-118, 1944, by H. K. Markey et al.

Permission granted for personal use.

August 1941

In their U.S. Patent No. 2,202,387 invention, Aug. 11, 1941 left, actress Hedy Kester Markey (Lamar) and composer George Antheil reveal a technique for guiding torpedoes to their targets by varying the frequencies of signals that control the torpedoes’ left (L) and right (R) movements. Variables such as form and other frequencies are determined by spinning seven different capacitors (left and 34). To a constantly varying pattern controlled by seven per torpedoes a paper strip similar to those of player-piano rolls. The inventors noted the variations in their career 1944, left bottom). Demonstrating her patriotism in yet another way, Markey mounted a poster calling for purchase of war bonds in her Beverly Hills home (circa 1945, top).
Putting the story together

Spectrum is grateful to Robert Price, chief scientist with M/A-
COM Linkabit, Inc., in Lexington, Mass., whose support was in-
strumental in bringing this fascinating story together.

Stimulated by spread-spectrum pioneer Paul S. Green, Jr.,
at present with IBM's Thomas J. Watson Research Center
in Yorktown Heights, N.Y., by University of California
researcher and teacher Robert A. Scholtz in Los Angeles, Dr.
Price undertook about five years ago to study and document
the evolution of spread-spectrum technology as many once-
secret documents became declassified.

Dr. Price, a dedicated communications engineer and a Fol-
low of the IEEE, sees his entirely voluntary effort as "replaying
a luckily incurred debt" to all those pioneers with whom he
worked in the early days of spread spectrum.

Searching for authentic sources, Dr. Price interviewed such
U.S. generals as Mark Clark, now deceased, plus others who
are still alive. Civilian interviewees included famous actress
Hedy Lamarr, whose torpedoes-guidance invention (see
"Screen star derails a frequency-hopping scheme," p. 76) Dr.
Price found to be "complete in its policy" antijamming con-
cept even before Pearl Harbor. During Dr. Price's interview
with her, Miss Lamarr autographed the accompanying photo,
taken at her Benedict Canyon home in California in 1941, dur-
ing her work there with composer George Antheil on their
common invention.

Dr. Price also recalls how Colonel Dorothy L.
Masten of Chicago, Ill., chief operator of the Pen-
tagon's SISYLL conference
room, volunteered that she had aided Presi-
dent Truman in his transatlantic
discussions with Prime Minister Winston
Churchill of His Majesty's peace offer—another
highlight in his research.

Dr. Price style is indebted to, among others, Arno E. Joel
of AT&T Bell Laboratories in Holmdel, N.J. Robert M. Farno
of the Massachusetts Institute of Technology in Cambridge,
and Claude E. Shannon of Western Mass., for their help
during his research.

Dr. Price also sees his close work with the late William R.
Bennett, important contributor to Bell Telephone Laborato-
ries' SISYLL secret telephone system discussed in the main
article, as well as with author David Kahn and Dr. Scholtz, as
an "outstanding privilege."

—Ed

later, "All right, then you notify Stalin, and I shall do the same
immediately, of this conversation between us."

"Exactly," said Churchill. And they rejected Hitler's offer.
Thus, the very end of the war, SISYLL played a role of
high importance in keeping secret the top plans of key leaders. It
ensured so much so well that the older A-3 scrambler, which
continued in service, carried relatively few communications of
importance. A German Foreign Office official noted dispa-
tionaneously on a sheet of Deutsche Reichspost intercepts that
"There is in general not much to be gotten from them." And
Marshall, whose refusal to use the scrambler in the morning of
Dec. 7, 1941, had had such dire consequences, was able to say,
three years later, probably with SISYLL in mind, that "we have
the very finest equipment now."

To probe further

Basic technical information about SISYLL and its develop-
ment may be found in M.D. Fagin, ed., A History of Engineer-
ing and Science in the Bell System: National Service in War and
Peace (1925-1975) (Bell Telephone Laboratories, Murray Hill,

The administrative and operational history of the military
agency that served SISYLL is given in the manuscript "Unit
History: Radio Signal Service Company," Box 5704, Record
Group 447, National Archives Records Center, Suitland, Md.,
1974. A larger view, though with fewer details, may be found in
Mary Louise Muffa's manuscript, "Signal Corps Fixed Com-
 munications in World War II: Special Assignments and Tech-
niques," April 18, 1946, War Department Special Staff,
Historical Division, in the U.S. Army Center for Military

Anecdotes about the use of SISYLL and transcripts or recol-
elctions of the conversations are in Vol. 1 of Harry S. Truman's
Memories (Garden City, N.Y.: Doubleday, 1954), pp. 89-94, and
Franklin D. Roosevelt, Escape to Adventure (Boston: Little, Brown,
1949), pp. 343-45.

Details about Alan Turing's contribution to SISYLL and
speech encryption are in Andrew Hodges's outstanding biog-
raphy, Alan Turing: The Enigma (New York: Simon & Schuster,

Information about German interception of the transatlantic
scrambler is in David Kahn, The Codebreakers (New York: Mac-

On spread spectrum itself, see Spread-Spectrum Communi-
cations, ed. by Charles E. Cook, Fred W. Ellerick, Lawrence B.
Miletin, and Donald L. Schilling (New York: IEEE Press, 1983),
a collection of articles; and the forthcoming Spread Spectrum
Communications by Marvin K. Simon, Jim K. Omura, Robert
A. Scholtz, and Barry K. Levitt (Rockville, Md.: Computer Sci-

Broadband invention rights to a basic spread-spectrum method
are now claimed by the International Telephone and Telegraph
Corporation, Nuremberg, N.J., in Reissue Patent No. 299,469, filed
Sept. 4, 1981. This U.S. patent reinforces application concerns the
original invention of L.A. deRose and Monnier Rogoff.

A receiver, dubbed Rake, that significantly improved the FIC
spread-spectrum system by comparing ionospheric multipath
interference was described in "A communication technique for
multipath channels," by R. Price and P. E. Green Jnr., in the Pro-

In his book Bodyguard of Lies, Toronto, New York, London,
1984, fourth ed., author Anthony Cave Brown says that Churchill
was warned by the British intelligence about Germany's breaking
of the A-3 scrambler.

Nearly 200 messages, including letters, telegrams, and tran-
scripts of telephone conversations between Winston S. Churchill
and Franklin D. Roosevelt are included in the three-volume book
Churchill and Roosevelt: The Complete Correspondence, edited
by Warren F. Kimball, to be published next month by Princeton
University Press of Princeton, N.J. The editor mentions
SISYLL in his introduction. The book includes 26 black and
white photos and 18 maps.

About the author

David Kahn is best known as the author of The Codebreakers
(Macmillan Publishing Co., 1967), now in its tenth printing. His
Hilar Spies was published also by Macmillan, in 1978. A found-
er and editor of Cryptologia, Dr. Kahn is an assistant editor
with Newsday in Melville, N.Y. He writes about cryptography
for many publications. Kahn on Codes, a collection of some of his
articles, was published in January by Macmillan. He holds a
Ph.D. in modern history (1974) from Oxford University.