(5)

FBI LAW ENFORCEMENT BULLETIN

JANUARY 1985, VOLUME 54, NUMBER 1

MHC
EMC

Contents

The Cover: Confrontations with irrational, violent individuals are day-to-day occurrences which threaten the safety of police officers everywhere. (Staged training photo.) See article p. 1.

Federal Bureau of Investigation
United States Department of Justice
Washington, DC 20535

William H. Webster, Director

The Attorney General has determined that the publication of this periodical is necessary in the transaction of the public business required by law of the Department of Justice. Use of funds for printing this periodical has been approved by the Director of the Office of Management and Budget through June 6, 1988.

Published by the Office of Congressional and Public Affairs, William M. Baker, *Assistant Director*

Editor—Thomas J. Deakin
Assistant Editor—Kathryn E. Sulewski
Art Director—Kevin J. Mulholland
Writer/Editor—Karen McCarron
Production Manager—Jeffrey L. Summers
Reprints—Regena E. Archey

ISSN 0014-5688 USPS 383-310

97483

Criminal Codes and Ciphers
What Do They Mean?

By
JACQUELINE TASCHNER
Cryptanalyst
and
ARTHUR R. EBERHART
Special Agent
Laboratory Division
Federal Bureau of Investigation
Washington, DC

Cryptology, the study of secret writings, covers a broad spectrum of human activity. As long as man has been able to read and write, he has wanted or needed to keep some of these writings secret. Whatever can be written can be encrypted, abbreviated, over simplified, or just plain mangled. However, the services of a cryptanalyst may be required to determine the meaning of these writings.

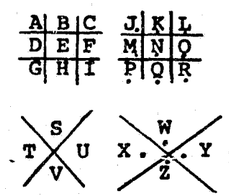
The FBI Laboratory examines such puzzles, ranging from highly sophisticated cipher systems to documents containing "meaningless" cryptic notations. Laboratory personnel apply the principles of cryptanalysis not only to clandestine business records related to gambling but also to suspected criminal documents from prostitution, loansharking, and drug cases. These specialized examinations are a blend of cryptanalysis and analysis based on specific knowledge of different illicit business transactions.

Examination of Criminal Documents

Most "bookie codes" are simple substitution codes. The bookmaker disguises the true meaning of his records by simply substituting an abbreviation, symbol, and/or shortened form of the word or words. For example, a horse bookmaker may record wagers placed on different horse races at New York's Aqueduct Racetrack by merely using the horse's numbers, race numbers, and the letter "A." The notation "3A7 2 JD" would represent a $2 wager made by John Doe on Horse #7 running in the third race at Aqueduct. (See fig. 1.)

Sports bookmakers often record sports wagers using the team numbers printed in different sports publications. For example, the notation "14-500" seen in figure 2 means a $500 bet was placed on the Philadelphia Stars.

Bookmakers have also relied on a very old "masonic cipher" to disguise important information as unintelligible symbols. This system uses two tic-tac-toe diagrams and two "X" patterns to represent the letters of the alphabet:



When a bookie enciphers the name "Harry Smith" using this system, it appears as:

HARRY SMITH

While an investigator may be baffled by these symbols, a trained cryptanalyst could decipher it with little effort.

Besides these simple substitution ciphers, gambling jargon, which itself is a form of code, can be decrypted by a cryptanalyst. Solving these simple codes is based on the common characteristics of gambling records, fundamentals of cryptanalytic procedure, and the use of reference materials, such as the *Daily Racing Form* and sports schedules.

Concealing bettors' and other bookmakers' telephone numbers has long been a major concern of illegal bookmakers. If most of the telephone numbers are from the same town having a single telephone prefix, deleting the first two digits of the telephone number may be enough to fool the untrained eye of the investigator. For example, Harry Smith's telephone number, 752-0321, in Wellstown will be recorded as "20321." The bookmaker knows that all the Wellstown prefixes are 752.

A more complex telephone number cryptosystem uses an additive (a series of numbers added to one or all of the digits in the telephone number). For example, a series of 1's

"As long as man has been able to read and write, he has wanted or needed to keep some of these writings secret."

Figure 1 Horse race bets

JD
3 A 7 2

John Doe (Bettor)

Wager
3rd race at Aqueduct
Horse #7
$2.00 to win

MS
4 B 3 44

Mary Smith (Bettor)

Wagers
4th race at Bowie
Horse #3
$4.00 to win, $4.00 to place

5 B 1 222

5th race at Bowie
Horse #1
$2.00 to win, place and show

7 B 9 XX2

7th race at Bowie
Horse #9
$2.00 to show
(no win or place bets)

(16)

$16.00 total wager

can be added to the telephone number given for Harry, making the notation in an address book "Harry 863-1432." However, that number could be nonexistent, and the investigator would not easily associate this phony number with the true bettor, Harry Smith, without the help of a cryptanalyst.

The telephone itself provides a simple substitution system which the bookie can use to record telephone numbers. One of three letters printed above a digit may be used to represent that particular number. However, since "1" and "0" have no such designations, the letters "Q" and "Z," respectively, are used as cipher equivalents for these digits. (See fig. 3.) This system provides variants which help disguise the substitution process. Thus, Harry's telephone number, 752-0321, would be recorded as "PJAZECQ."

A more-sophisticated telephone number encryption system uses a 10-letter keyword having no repeated letters. One letter is substituted for each digit from 1 through 0. Using the keyword "CUMBERLAND," the bookie will encipher Harry's telephone number as "LEUDMUC:"

Keyword	C U M B E R L A N D
Digits	1 2 3 4 5 6 7 8 9 0
752-0321	Harry's true telephone number
LEU DMUC	Encrypted number found in the bookie's notes

The cryptanalytic attack on records containing such enciphered telephone numbers involves identifying the 10 letters, LEUDMC plus ABNR (developed through other tele-

Figure 2

Week Eight
Saturday, April 14

Score			1	2	3	4
	1	Oklahoma 11:30P 1:30C 2:30E 8:30H				
	2	Washington				
	3	Memphis 5:00P 7:00C 8:00E 3:00H				
	4	Los Angeles				
	5	San Antonio 5:00P 7:00C 8:00E 3:00H				
	6	Jacksonville				
Sunday, April 15						
	7	Denver 11:30P 1:30C 2:30E 9:30H				
	8	Pittsburgh				
	9	Arizona 11:30P 1:30C 2:30E 9:30H				
	10	New Jersey				
	11	Birmingham 11:30P 1:30C 2:30E 9:30H				
	12	Michigan				
	13	Chicago 11:30P 1:30C 2:30E 9:30H				
	14	Philadelphia				
Monday, April 16						
	15	Houston 8:00P 9:00C 9:00E 4:00H				
	16	Oakland				
	17	Tampa Bay 8:00P 9:00C 9:00E 4:00H				
	18	New Orleans				

Figure 3 Telephone dial and letter equivalents

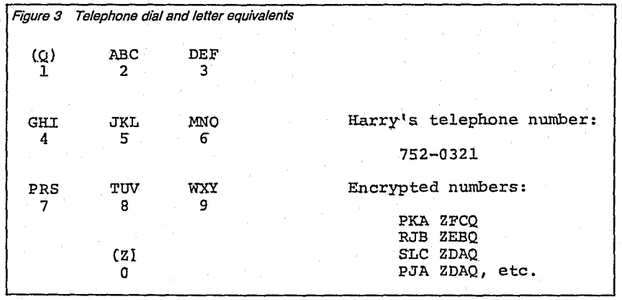
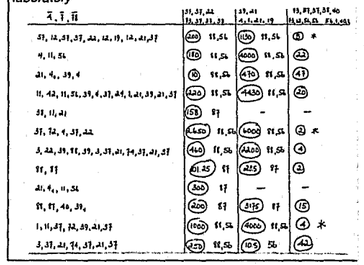


Figure 4 Portion of evidence seized in PCP laboratory



phone numbers). These 10 letters are then anagrammed (rearranging the letters to form a readable word or words) by pairing letter combinations frequently used in the English language, such as ER and AND. Through trial and error, the cryptanalyst will anagram the correct keyword. Proof of the accuracy of the keyword comes from the criss-cross directory [1] and local telephone books.

Examination of Drug-related Records

Keyword systems for telephone numbers are not limited to illegal gambling operations. In a drug-related money laundering scheme, investigators sent telephone address books containing strange notations to the FBI Laboratory for analysis. The documents were suspected of containing telephone numbers of individuals involved in the operation. Subsequent examination determined the letters of the keyword, MONEYTALKS, were used to represent the digits 1 through 0. The decryption provided valuable investigative leads useful in breaking up this operation.

A more-complex substitution system was used in a drug case in which a chemist tried to disguise the records of his clandestine phencyclidine (PCP) laboratory. When Drug Enforcement Agency agents raided the laboratory, they located notebooks containing page after page of one- and two-digit numbers. (See fig. 4.)

From the decryption, a chart could be constructed showing the relationship between the numerical cipher text equivalents and the plain text letters. This substitution chart was:

1	3	11	19	37	55	87	4	12	20	38	56	88
A	B	C	D	E	F	G	H	I	J	K	L	M
21	39	57	89	22	40	72	23	41	73	24	42	74
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

With this information, the cipher is readable, but the analysis was only partially completed. The reconstruction of the key (used to remember the system) was then required. Analysis of the substitution numbers revealed a pattern when the numbers were regrouped as follows:

1
3 4
11 12
19 20 21 22 23 24
37 38 39 40 41 42
55 56 57 72 73 74
87 88 89

With these types of patterns, the cryptanalyst must focus on the case to determine why they occur. Since this was a drug case involving a chemist, chemistry or chemicals would be a good starting point. With a little research into basic chemistry, the pattern was found to resemble the structure of the standard Periodic Table of Elements. The "atomic numbers" of the elements in the first column are the same as the first seven equivalents in the cipher alphabet:

Atomic Number	1	3	11	19	37	55	87
Letter	A	B	C	D	E	F	G

The atomic numbers for the first six columns of the periodic table were used as the key for the ciphers. (See fig. 5.) A periodic table hanging on the wall by the chemist's workbench supported this hypothesis.

Even so, examination of this material had yet to be completed. The decrypted notebooks contained detailed records concerning the scope and financial picture of the illegal PCP manufacturing operation. These documents revealed:

1) The various chemicals used to make PCP,
2) The actual quantities of each chemical needed per batch,
3) Notations indicating that one batch of PCP was made per week,
4) The current inventory of chemicals,
5) Calculations of how long the supply of each chemical would last,
6) What chemicals were "on order" and from which chemical suppliers,
7) Dates that chemical orders were sent and anticipated delivery dates,
8) A cost breakdown per batch of PCP (by individual chemical price),
9) Notations for "rent" ($100) and the chemist's "minimum salary" ($1,000), and
10) Profit calculations per batch, based on a minimum sale price of $800 per lb.

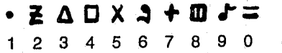
These financial records were also compared to other accounting records found during the investigation. The common notations were traced through three separate accounts, indicating a conspiracy.

As can be seen, a drug importer or dealer disguises the true meaning of his records in the same way as a bookie—by simply substituting an abbreviation, symbol, and/or shortened form of a word or words. The record of a drug sale usually would not contain the clearly incriminating message, "One kilogram of cocaine sold to John Doe for $58,500 on January 1, 1983." The record might more commonly be written "1k JD 58.5 1/1."

Cryptanalysts are able to derive a wealth of information from the jottings of a drug dealer or trafficker. They can tell what kinds of drugs are involved in the operation, the extent of the operation (the quantity of drugs involved, the number of people involved, and the amount of profit obtained), possible evidence of a conspiracy, and other information that may be useful to the investigator.

Prosecutors also benefit from this information as well. In one case, a man accused of dealing heroin claimed he was only a user. When the transaction records were submitted to the FBI Laboratory for examination, the cryptanalyst determined that the accused had bought over 7,000 "bindles" of heroin, worth almost $500,000, in just a 6-month period. Thus, the cryptanalyst's testimony in court was helpful in successfully prosecuting the man as a dealer, not a mere user.

Sometimes ledgers and records cannot be identified as drug-related because they are incomplete or sparse. For example, three encrypted ledger pages were sent to the FBI for examination. The ledgers contained a simple substitution cipher, where the digits in the ledger were replaced by symbols in the following manner:



While the cryptanalyst was not able to say that the records were the type found in a cocaine-trafficking operation, subsequent testimony revealed the clandestine nature of the records and the criminal intent (by concealment) of the defendant.

There is not always a one-to-one relationship between the symbols or letters in a ledger and the digits they represent. Sometimes, a character can represent a specific amount. For example, figure 6 shows a piece of paper seized in a prostitution investigation. When decrypted, the following equivalents were found:

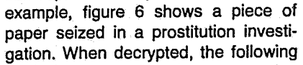


Figure 5 The periodic table of the elements

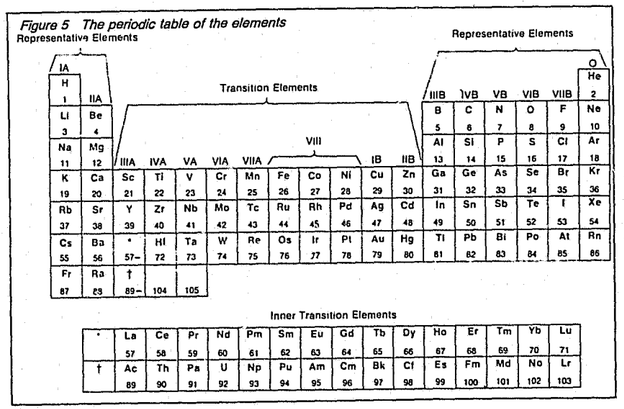
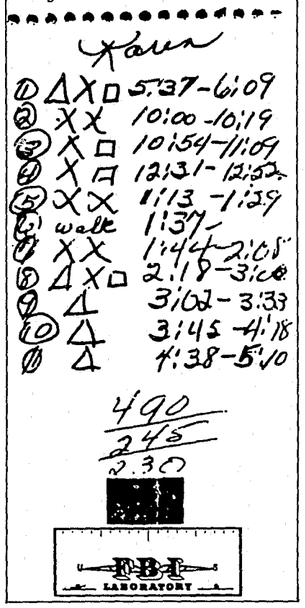


Figure 6 Scrap of paper seized in prostitution investigation



The remaining records were analyzed to determine the scope of the business, the number of employees, their roles, and the gross and net revenues. The "490" shows the amount of money earned by "Karen," half of which was given to the "house." From the $245 Karen earned that day, $15 was paid to rent the room, a notation that consistently appeared in the records.

Occasionally, mysterious notations are completely innocent. When investigating a theft of valuable antiques, police found the following strange notation on the front door of the house adjacent to the burglary location:

HFIOIR
ATMHCE
OPLOLS
ETC-TI
ISN$G6
50

Some clever paperboy almost became implicated in the crime. However, when deciphered by rearranging the letters, the note read: HI I AM COLLECTING FOR THE POST—IS $650 (sic). This is a variation of the "rail fence" cipher, so named because the plain text resembles the slats of an old rail fence when completely written out.

Conclusion

Investigative personnel are encouraged to consult with a cryptanalyst regarding dubious records or documents. Cryptanalysts do more than work on the conspicuous, unintelligible jottings of a criminal. Major conspiracy networks, like all organizations, depend on communications. Because of the illegal nature of the work, the correspondence may be disguised by a cipher system, and the cryptanalyst could help an investigator to get the full value of evidence obtained.

Because of the unique nature of the examinations and services provided by the FBI Laboratory and the variety of evidence which may be encountered, it may be appropriate to contact the Laboratory to resolve any questions which arise by writing:

Director, FBI
Attn: Laboratory Division
Document Section
Washington, DC 20535

The services of the FBI Laboratory are available to all Federal agencies, U.S. attorneys, and military tribunals in both criminal and civil matters. These services are also available to all duly constituted State, county, and municipal law enforcement agencies in criminal investigative matters. Expert witnesses are also available to testify in judicial proceedings.

FBI

Footnote

A criss-cross directory is a book which lists information on published telephone subscriptions. The directory is often organized in three parts: By telephone number, subscriber, and address. These three sections can easily be cross-referenced to yield other investigative information.

END