Criminal investigations in cryptology during the lifetime of Annibale Fagnola.

Journal of Criminal Law and Criminology

Volume 26
Issue 6 *March-April*

Article 10

Spring 1936

Cryptography in Criminal Investigations

Don L. Kooken

Excerpt below.

POLICE SCIENCE

Editor: FRED E. INBAU

CRYPTOGRAPHY IN CRIMINAL INVESTIGATIONS

DON L. KOOKEN†

Considerable misapprehension has been present as to the importance of cryptography in criminal investigations. Most investigators are of the belief that cryptograms are seldom encountered in ordinary criminal investigations and that to become proficient in the solution of cipher writings one must have a special aptitude for the work and spend years in training on the subject. They conclude, therefore, that it would be inadvisable to devote a considerable length of time to a study of cryptography. Experience has taught us that these beliefs are ill-founded. It is true that cipher experts such as Major Herbert Yardley, Colonel George Fayban and Colonel Parker Hitt, have devoted many years in the study of complicated military ciphers and codes, and that to become expert in the class represented by these gentlemen would require what Major Yardley chooses to call "cipher brains." However, any person of ordinary intelligence and endowed with a stubborn perseverance can, by careful analysis, solve the simple type of cipher commonly encountered in criminal investigations.

> "The investigating officer who would decipher secret writings must have his heart in his work, perseverance, never-failing interest, an observation that allows nothing to

†Supervising Lieutenant, Indiana State Police.

> escape, and the gifts of combination and deduction. These are indeed general qualities which every investigating officer ought to possess. One might almost say that every man who is of the stuff out of which investigating officers are made is capable of reading ciphers."[1]

Cryptograms are encountered in criminal investigations much more frequently than one would imagine; often, however, they are not recognized as such. If the investigator will carefully scrutinize the notes, memoranda, letters, etc., of a criminal suspect, enciphered documents may be brought to light which otherwise would have gone undetected. A letter seemingly devoid of sense, a note book containing what appears to be pages of meaningless numerals, or an apparently insignificant scrawl on the back of an envelope, may prove to be secret writings, and though little importance is attached to it at the time, if deciphered, the result may alter the entire investigation. Of course, ciphers will be found which, after decipherment, may have no immediate bearing upon the case, but it must always be borne in mind that anything of sufficient importance to be enciphered is likewise of sufficient importance to be deciphered.

The complex operations of organized criminal bands necessitate the keeping of records, and of communication by telegraph and by mail. To protect these records and communications from exposing the nature or extent of the operations of the band should they fall into the hands of the police, ciphers are resorted to. The cipher writings taken from an arrested bank robber may disclose upon decipherment the names and addresses of his associates; the enciphered note book of a thief may, upon solution, prove to be a record of the fences through whom the thief disposes of his loot; and enciphered telegrams and letters may provide the connecting link in working up conspiracy cases.

The old adage "there is nothing new under the sun" is particularly applicable to cryptography. Nearly everyone has at one time or another made use of secret writing. He may have altered slightly a method or system of which he has read or he may have set about to devise a system of his own, but invariably when the non-expert invents a cipher, without knowing it he makes use of a system that has been in use since the reign of Julius Caesar or even before that time, for the origin of cryptography is obscure. History is replete with incidents of the use of cryptograms, and traces of its use pene-

[1]Gross, H., Criminal Investigation (3rd ed., Adam's Trans'l.—Kendal, 1934) 390.

trate the ages until they are lost in the mists of antiquity. It may be assumed, however, that hardly had writing as a means of recording thought been invented when there arose the necessity for evolving a method of writing that would be unintelligible to all except the person for whom the message was intended.

The ciphers encountered in criminal investigations are usually those of the non-expert and the problem of the investigator is to determine the basic principles of the system used and the method of analysis to follow in arriving at a solution. It is the intent of the writer to set out in this article simple rules of classification and analysis, to enable the investigator, with a reasonable amount of study, to recognize the simple types of cipher and proceed intelligently to their solution. For those who desire to attain proficiency in deciphering the more complex ciphers there are many excellent books available.[2]

The method or system of secret writing is called "cipher" and the enciphered message is referred to as a "cryptogram." Codes are arbitrary ciphers; that is, a word or a group of letters is given an abitrary meaning, usually more or less extended. While the sole purpose of ciphers are to preserve secrecy, codes are primarily used to condense messages for transmission. Very elaborate codes are used by governments and by many commercial institutions for the dual purpose of secrecy and economy in transmission. Codes, however, are not adaptable to the needs of the criminal, principally by reason of the hazard of written code books or keys falling into the hands of the police, although some very elementary codes have been encountered in criminal investigations. For practical purposes the criminal requires a system of enciphering that can be easily memorized, that can be frequently changed, and one that is not so involved as to make its use inexpedient.

Cryptograms may be roughly divided into two classes: transpositional, and substitutional. In the former class the letters or words of

[2]See the following, which also constitute the bibliography for this paper:
(a) De Grandpre, A., La Cryptographic Pratique (1905);
(b) Givierge, M., Cours de Cryptographie (1932);
(c) Hitt, P., Manual for the Solution of Military Ciphers (1918); also see Hitt, The A, B, C of Secret Writing (1935);
(d) Josse. H., La Cryptographie et ses Applications a l'art Militaire (1885);
(e) Kasiski, F. W., Die Geheimschriften und die Dechiffrir-Kunst (1863);
(f) Kerckhoffs, A., La Cryptographie Militaire ou des Chiffres Usites en Temps de Guerre (1883);
(g) Langie, A., Cryptography (1922); also see Langie and Soudart. Traité de Cryptographie (1935);
(h) Thomas, P. B., Secret Messages (1929);
(i) Valerio, P., Essai sur les Methodes de Dechiffrement (1893);
(j) Von Wastrowitz, E. B. F., Handbuch der Kryptographie (1881);
(k) Yardley, H. O., The American Black Chamber (1931).