5 April 1955

The Basic Principles of Cryptanalysis

The problem of understanding a message which was not directed to one, and which is in fact intentionally obscured, is a broad one and has arisen in many fields, including the baseball diamond. It has reached its greatest difficulty and evoked the most ingenuity in solution in the field of military communications.

My object in this note is to point out some basic principles. There may be other ways of stating these principles, and there may be other principles besides, but these are basic in the sense that they cannot be circumvented.

In simple terms an interceptor B is listening to transmissions sent from A to C, who are taking pains to keep B in ignorance. The only possible way that A and C can hope to succeed is to utilize some background information which is unknown to B. Generally this is prearranged material called "key". The message then fits into this background to make a coherent statement.

This is principle number one; communications A and C must have some information not available to the interceptor.

If the link from A to C is to have utility it must be able to accommodate any messages from a large bank of possibilities, and accommodate these in large volume. It is not possible for A to assert in advance what messages from this bank he will send nor in what number. If it were possible, the communications link would not be needed.

The messages to be sent are not under the control of the communicator. A; he must take all comers. His key must have similar properties; it must

be unpredictable.

If his keys are all from a clearly defined subset then the cryptanalyst B, once he recognizes this fact, has an excellent chance to recover information. For instance, suppose the key were digits to be added to digital plain text, and that the key had no zeros in it.

This is the second principle. If the key comes from a subset which does not allow almost all the possibilities, then the cryptanalyst will eventually read some of the messages.

The set of possible keys may have another weakness. If the key can be represented as a combination of sub-keys in such a way that this representation carries through the encipherment, then the cryptanalyst can deal merely with a sub-key. An example is the Hagelin C-38, where the key is the result of contributions from 6 different wheels. Solution is frequently achieved by attacking one of these wheels at a time.

Principle number three is this. If the keys can be split such that the split carries through the encipherment, then the cryptanalyst can attack one part at a time. The cryptographer A is playing a game, in the mathematical sense, with the cryptanalyst B. The game is such that the gain of one is not necessarily equal to the loss of the other. The game has significant chance elements, the message source and the risks they may encounter en route (busts). Player A must select his strategy in advance, and is on the defensive; he cannot afford mistakes. Player B can improvise his strategy as new information becomes available; he is on the offensive. The fact that this is a game explains the formidable complexity encountered in any attempt to catalog cryptanalytic attacks. This complexity is frequently met in detailed prescription of a strategy.

The fourth principle is: the choices open to A and to B define game strategies, in which the effectiveness of each depends upon the actions of the other.