[redacted] DECLASSIFIED NRL REPORT 3542

[redacted]

FR-3542

IFF REPLY CODING

[redacted]

NAVAL RESEARCH LABORATORY

WASHINGTON, D.C.

[redacted]

ADDRESS REPLY TO
DIRECTOR, NAVAL RESEARCH LABORATORY
WASHINGTON 20, D. C.
AND REFER TO:

S-2000-13/50 brg
Ser. 7373

NAVAL RESEARCH LABORATORY
WASHINGTON 20, D. C.

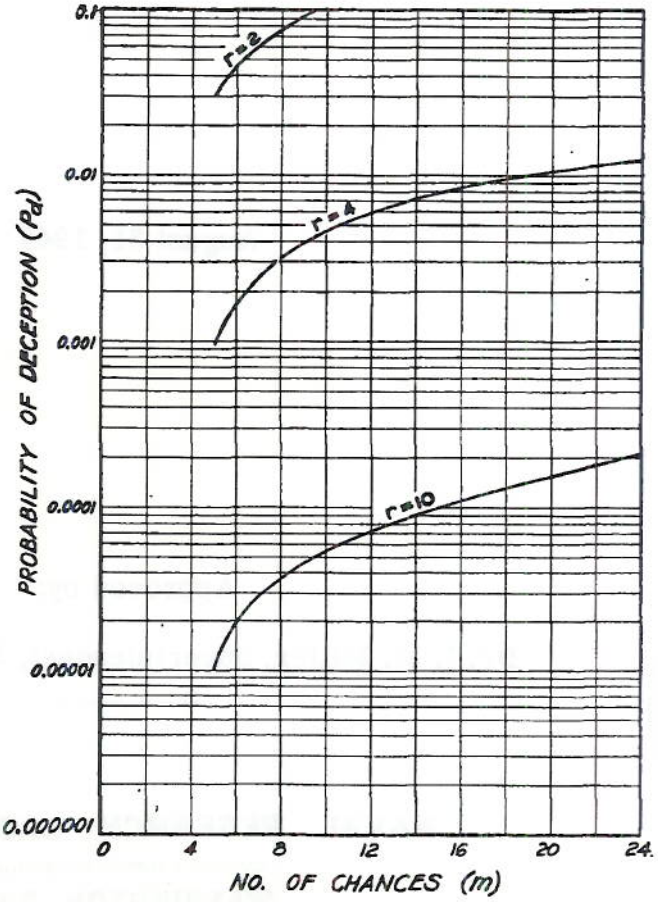
26 January 1950

[redacted]

From: Director, Naval Research Laboratory
To: Distribution List

Subj: NRL Report 3542, "IFF Riply Coding" (Secret); correction of

1. Figure 6 on page 9 of subject report should be corrected as follows:



F. R. FURTH

M. E. Jansson

M. E. JANSSON
By direction

IFF REPLY CODING

C. E. Cleeton

August 31, 1949

Approved by:

Dr. J. M. Miller, Superintendent, Radio Division I

NAVAL RESEARCH LABORATORY
CAPTAIN F. R. FURTH, USN, DIRECTOR
WASHINGTON, D.C.

CONTENTS

ABSTRACT

In a transpondor type of IFF system, cryptographically coded, deliberate garbling of the code by an enemy to appear friendly must not be permitted. To prevent this, frequency-coding is more satisfactory than pulse-coding, but the latter may be suitable for the auxiliary function of aircraft control. The probability of deception by guessing the correct code is computed for several system designs, and it is shown that a relatively small number of reply codes is ample to make this probability low if appropriate integration of replies is required before deciding that the indication is friendly.

PROBLEM STATUS

This is an interim report on the general IFF program.

AUTHORIZATION

NRL Problem R03-06R
NR 527-006
BuShips Problem S1234X-S

[redacted]

IFF REPLY CODING

INTRODUCTION

From an IFF viewpoint, the primary function of an IFF system is to distinguish friend from foe. As a consequence of the expected increased speeds of planes and missiles, a system meeting future military requirements must provide a type of security which will enable hostile targets to be recognized without dependence on human judgment. Further, the system must provide the required information rapidly. Accomplishment of such a system is important because an enemy may possess super weapons of such a nature that he could well spend considerable effort to appear as a friend in order to deliver a single missile. The IFF data should be supplied as rapidly as the detection data. In terms of conventional search radar characteristics, this means recognition during a single sweep of the antenna past the target.

Security by concealment of techniques, which has been so largely relied upon in the past, is an unsatisfactory approach because concealment and effective combat use are incompatible. A satisfactory and more permanent solution to this security problem is promised by utilizing a cryptographic method of coding applicable to an IFF system.

The correlation of IFF with detection data is accomplished by comparing the position coordinates of the target as measured by the two systems. Thus, the IFF system must supply one or more position coordinates of the detected object. Further, it must be some form of communication system which will permit a cryptographic encipherment of certain intelligence to be transmitted. It is conceivable that an IFF system could be developed in which, upon request or periodically on a prearranged schedule, the friends transmit their position coordinates to any location desired. Then if these communications were securely enciphered, one might expect to have accomplished the security required. However, the ease of correlation of position coordinates, when radar methods are used for IFF as well as for detection, makes the conventional interrogator-responsor-transpondor system more attractive.

On the other hand, the enciphering problem becomes somewhat different from the familiar communication problem. We no longer have a large number of variegated messages to transmit (the position coordinates of a single plane being a message) but instead have a single message in the form of "Are you a friend?" with a reply "Yes." The cryptographic problem in reply coding is one of finding a way of saying "Yes" that cannot be copied by an enemy. This may be accomplished by providing a large number of reply codes from which the answer is selected. Because an enemy can monitor all transmissions, the same combination should not be repeated once an interrogation is made and the reply received. A new arrangement should be used for the next interrogation. Since the enemy may interrogate our transpondors with one interrogation after another, we must provide a number of interrogation codes large enough to make this approach impracticable for him.

[redacted]

If, for any one brief interval of time, we authorize a single interrogation and associated reply, change to a new randomly selected combination for the next interval, and so on, we might accomplish adequate security. This, however, imposes a tremendous problem in synchronization of code selection for all equipments. An alternative which has been proposed[1] is to provide an arrangement such that each of the large number of interrogation codes has associated with it a predetermined reply. Interrogations are individually selected at random, but no synchronization is required for there will be one and only one reply authorized for any interrogation selected. The device which determines the association between interrogations and replies must be changed at frequent intervals, just as it would be necessary to change the programming of the previous method. In the latter case, however, this change is required only because equipment may fall intact into enemy hands or the code may be discovered by analysis. Hence the interval between code changes may be of a different order of magnitude than in the former case in which the programming device must supply a rapid change of code.

There are also functions other than IFF which can be performed by an interrogator-responsor-transpondor system. It is attractive, therefore, to attempt a combination of functions into a single system in order to conserve equipment. Though these other functions may be extremely important, they will be referred to as auxiliary functions of an IFF system when so incorporated. It is the purpose of this report to examine in detail the security requirements of the reply code for the cryptographic system suggested, to discuss certain other requirements and restrictions that an IFF system places on the reply signal, and to comment on reply-code requirements which may be imposed by a decision to add auxiliary functions.

POSITION COORDINATE DATA

One or more position coordinates of the transpondor signal must be supplied in order that the recognition and detection data may be correlated. A single pulse response is adequate to supply range and azimuth data by use of the same techniques as used in radar detection systems. The third coordinate, if required, is less easily provided. Radar systems do not determine elevation (or altitude) accurately because of interference of surface-reflected signals. Likewise, elevation of IFF signals may be in error when determined by direction-of-arrival methods. If the system is to be used only for recognition of friends or foes, these errors would be unimportant provided the relative error was sufficiently small. However, since it would be clearly impracticable to place all radars and the IFF on the same frequency, the relative errors would undoubtedly be greater than, say, the relative error in elevation between two targets close to each other, as measured by a single radar. Further, the technical difficulties of obtaining adequate vertical coverage and reasonably good elevation-angle determination at high data rates warrants an examination into the possibility of communicating the third position coordinate (altitude), when needed, as measured independently at the transpondor, to the interrogating site via the IFF reply channel. Fortunately, this coordinate is the easiest to determine at the transpondor because of the stable reference plane (earth's surface). Also, equipment-wise it may be satisfactory to use a simple aneroid capsule to supply the data.

If the altitude is measured at the transpondor, the reply code must be capable of communicating this data in the detail required. For IFF only, the detail required will be a function of the absolute accuracy of the detection radar. If the system is to be used for other purposes where only the IFF signals are being compared, the relative accuracy of measurement may provide the criterion for the detail to be transmitted.

---

[1] *Cleeton, C. E., "Proposed System of Electronic Recognition—Report of Progress II," NRL Report R-3433, (Secret), March 16, 1949.*

[redacted]

SUITABLE TYPE OF REPLY SIGNALS

A single reply signal cannot satisfy the security requirement. We are concerned with preventing the enemy from giving the authorized reply. Hence it is obvious that there must be at least two possible alternative replies from which he must make a choice. The simplest means of providing this minimum number is for the authorized reply to be either a signal or no signal. One objection to this, however, is that an enemy making no attempt to compromise the system would give a friendly indication half the time. Also, position data cannot be transmitted when "no signal" is the authorized reply, again normally about 50 percent of the time. It seems very probable that any system will be pressed to collect data at higher and higher rates as target speeds increase. Thus a no-signal reply code should be avoided. Therefore, two reply codes may be considered as the absolute minimum. The desirability of a greater number will be considered later. If auxiliary functions are to be provided by the IFF system, a number of reply codes may be required to carry related intelligence.

In an interrogator-transpondor system, the interrogation synchronizes the replies of all transpondors responding. If a number of transpondors are in the interrogating beams, they will, in general, reply. If they are about the same range from the interrogator, the replies will occur at about the same time. The reply signal must necessarily extend over some short period of time, so that these synchronized replies may very well overlap. The greater the duration of the reply, the greater the probability of overlap. Moreover, in formation flying of planes, there is a good probability that overlapping reply signals will occur in an IFF system in which all planes are producing the reply signal.

This condition will give rise to a garbling of certain kinds of codes such as a pulse group. Not only may wrong codes be generated by the composite signal, but any authorized codes that do exist in the signal may be masked. The solution of turning off all sets but one, when such grouping occurs, is not a good one because of the effort required to enforce such operational procedures.

Because a future IFF system should be capable of rapid identification under high traffic conditions, the signals should be such that the code may be determined electronically for all targets without the necessity of gating in any coordinate. On the other hand, if, for example, the carrier frequency of the reply is varied to establish the codes, garbling does not exist because the frequency characteristic of a signal is not destroyed by additional signals. And no processing of the video signal is required to establish the code. The signal is in a form suitable for entering the display or evaluation equipment. Such a frequency-coding for the reply path then has a definite advantage. The question is largely one of whether by this means, a sufficient number of codes can be produced in a manner suitable for such a system.

If the IFF system, in addition to supplying friend-or-foe information, must perform other functions and possibly communicate altitude data in considerable detail, it is likely that frequency codes alone for the reply will be impractical. Friend-or-foe determination is the primary function of an IFF system, and, since a system permitting garbling of the IFF code would allow an enemy to proceed using a deliberately garbled code (with the possibility that it was a result of two or more friendly planes in close proximity), garbling of the IFF reply must be avoided. But this does not necessarily restrict the type of codes used for auxiliary functions. One should examine the possibility of a combination of frequency- and pulse-coding where the pulse codes convey information other than the friend-or-foe signal.

For example, in a pulse group range-coded, the range is customarily indicated by the leading edge of the first pulse. The range measured to the nearest target would not be

affected by a garbled pulse code. The range resolution suffers under any form of range-coding. Thus, for close groups of targets, the group as a whole may be identified as friendly or hostile by the frequency code, but, because of poorer resolution, an enemy plane might be more likely to succeed as a snooper and follow our flight home. This situation applies to recoverable airplanes rather than to missiles, for it is unlikely that we would return our missiles to our base. If, then, our planes are piloted, they should be equipped to detect snoopers.

If pulse-coding is used for conveying altitude information and garbling occurs, correlation of the IFF and radar data is not necessarily lost, for the other position coordinates will in general be adequate for the purpose. However, if traffic control is an auxiliary function of the system, the necessity for determining altitude of planes in a stack may make pulse-coding impractical. While a thorough evaluation of pulse codes for auxiliary functions cannot be made without first specifying these functions, it would appear probable that garbling would not be serious in many cases. This would be true where such functions are applied to individual planes likely to be deliberately separated from other friendly planes. Examples would be traffic control in approach regions where such spacing is the purpose of the function, and aircraft direction where planes are usually involved individually.

SUMMARY OF REPLY-CODE CHARACTERISTICS

Thus we arrive at certain conclusions regarding the reply code which may at this point be summarized as follows:

a. A single pulse reply is adequate to provide range and azimuth information on the transpondor signal.

b. It may be advantageous to convey transpondor altitude data by reply codes.

c. Two or more reply codes are required for security reasons.

d. A no-signal reply is unsatisfactory because of count down of position data.

e. A garbling of the reply security-coding is serious, but it may be avoided by use of frequency-coding.

f. If auxiliary functions are provided, it may be necessary to provide additional reply codes of a different character than required for IFF.

g. Garbling of intelligence being conveyed for some auxiliary functions is not too serious and is less likely to occur when information is needed than in the IFF function. Thus, pulse-coding would be acceptable for certain auxiliary functions.

NUMBER OF REPLY CODES REQUIRED FOR SECURITY

The number of IFF reply codes required for security reasons will, in general, be a function of the number of replies which may be received from a transpondor before a friend-or-foe decision must be made and the probability of error that one is willing to accept. If the enciphering system is subject to successful analysis, the labor involved in making the analysis may be a function of the number of reply codes.

Suppose, however, that a cryptographic coding method has been devised which is not subject to analysis, to the extent that replies to future interrogations can be predicted from the results previously observed. In this case the enemy can only guess as to what reply is authorized for each interrogation he receives. We will first examine the probability of misidentification for the minimum of reply codes. As has already been pointed out, at least two reply codes must be available in order that the enemy may be forced to guess between alternatives. While one of these could be a no-signal reply, the count down of position data from our own transpondors is undesirable. Therefore, assume that there are two possible replies each consisting of a signal in which some characteristic, such as the frequency channel, is varied. We will, of course, have a third possible response to an interrogation—the no-signal response. This response will be obtained (1) from enemy targets that do not attempt a reply to the particular interrogation, and (2) from both enemy and friendly transpondors which, for some technical reason such as low signal strength or count down resulting from multiple interrogations, fail to reply to the particular interrogation. Although these failures should, except for unusual conditions, constitute a small percentage of responses, they will force us to design the system to allow for a certain number of failures to reply even when the target is recognized as friendly. This means that, on the average, several interrogations must be made and the composite response used to determine whether enough of the replies were correct to make the probability of enemy deception low.

There are several ways of building up the composite response:

a. A series of interrogations at the recurrence rate of the interrogator may be made on each sweep of the antenna beam past the target. Let m denote the number of interrogations during this sweep. The effective reply is the composite response to the m interrogations.

b. Each successive scan of the antenna will make a new attempt at recognition. If there is time to get these additional "looks" at the target, the probability of deception will be decreased accordingly.

c. Frequently more than one interrogator will be attempting recognition of the target. If the various sources of data are being coordinated, the probability of deception will be reduced correspondingly.

If we ignore the latter two conditions, letting them merely serve as safety factors, and design the system to be adequate to provide a good probability against deception when we have time to obtain only one "look" at the target with a single interrogator, our design will be conservative.

If the replies are presented directly on a PPI display, the decision as to whether the composite signal should be recognized as that of a friend or an enemy will be made by the operator. A variety of combinations of replies and misses may be presented for his judgment. If, however, the signals are evaluated electronically, practical decoders will accept only a limited number of arrangements which produce a friendly indication. The following conditions are typical of those which might be used:

a. If, out of a total of m interrogations, n or more replies are correct, a friendly response will be produced.

b. If, out of the m interrogations, n correct replies are received on successive interrogations, a friendly response will be produced.

[redacted]

c. If, out of l successive interrogations in m interrogations, n replies are correct ($n<l<m$), a friendly response will be produced.

If the individual replies are displayed directly on a PPI, recognition will be based upon the display of an adequate number of reply signals. Although any accurate estimate of the number required can only be determined experimentally from a statistical study of operator reaction, an analysis of condition (a) above will provide some information as to design requirements. For electronic evaluation, this method is merely a counting process and would require means capable of storing signals for several sweeps. The presentation would be delayed by a time corresponding to the number of interrogations required to build up n correct replies. Also, the probability of deception would vary with the antenna beamwidth, since m depends on it.

The second and third methods are particularly applicable to electronic evaluation. The techniques used in defruiting[2] are applicable to this problem of electronic integration of the individual replies to permit a friendly response to be indicated only after certain conditions have been met.

PROBABILITY OF DECEPTION FOR DIRECT DISPLAY

For the direct display of the signals on a PPI, the probability of deception will depend largely upon the percentage of correct replies presented. Even though electronic methods are used to reduce the number of friendly indications, it may be desirable to present several of these indications during a single sweep of the antenna, and the recognition will then be based upon the number of such indications. Accordingly, it will be useful to examine how the probability of guessing the correct reply varies with system parameters.

If the number of reply codes is r, the probability of guessing the correct reply (only one authorized at a time) is $p = 1/r$ for a single interrogation. The probability of not guessing the correct reply for a single interrogation is $(1-p)$. If succeeding interrogations are unrelated to those previously used, the probability of guessing correctly n times in succession is $p^n = (1/r)^n$. The probability of guessing correctly exactly n times out of m independent trials is a well-known theorem in probability.[3]

$$P_m(n) = C_n^m p^n (1-p)^{m-n} = \frac{m!\, p^n}{n!(m-n)!} (1-p)^{m-n} . \qquad (1)$$

The probability of guessing correctly n or more times out of m chances will be the sum,

$$P_m(\geq n) = P_m(n) + P_m(n+1) + \ldots\ldots + P_m(m) , \qquad (2)$$

or

$$P_m(\geq n) = 1 - \left\{ P_m(0) + P_m(1) + \ldots\ldots + P_m(n-1) \right\} . \qquad (2a)$$

---

[2] *Parsons, J. R., "IFF System Defruiting with a Mercury Delay Line," NRL Report R-3278, (Confidential) April 14, 1948.*

[3] *Fry, T. C., "Probability and Its Engineering Uses," D. Van Nostrand Co., New York, p. 63.*

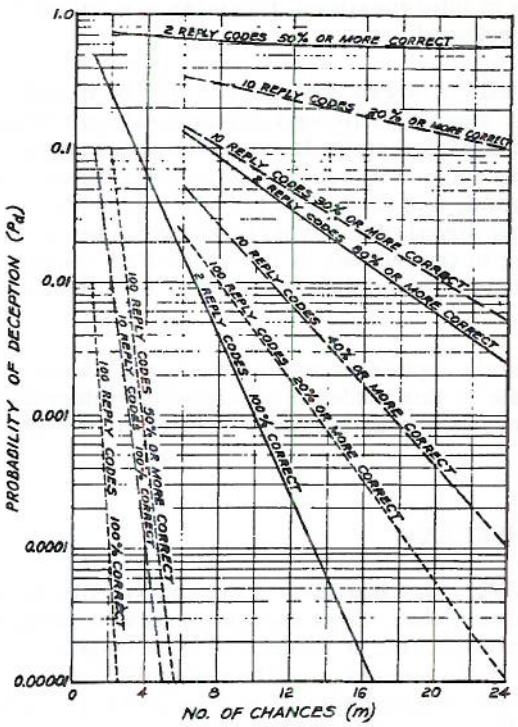


Fig. 1 - Probability of deception (P_d) for various percentages of correct replies in m successive chances (interrogations to which replies may be expected in a single beam sweep) for systems having r reply codes

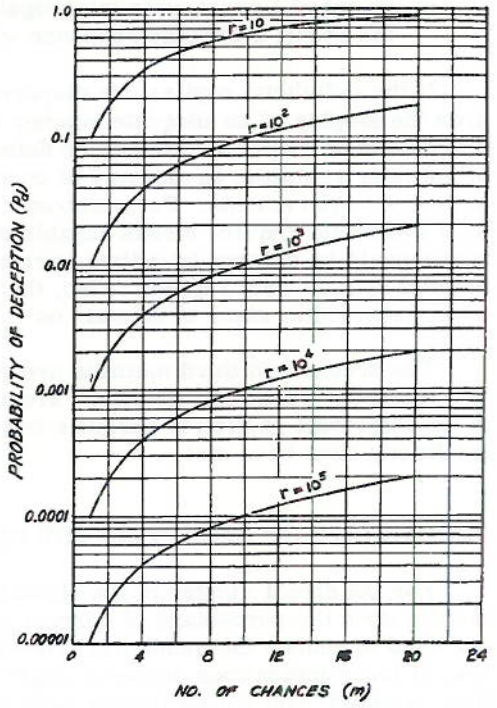


Fig. 2 - Probability of guessing at least one correct reply in m chances. No. of reply codes from which the correct one must be chosen = r

We will denote by P_d the probability that an enemy could, by guessing the correct code, deceive us to appear as a friend. Figure 1 is a plot of P_d against m for values of r as indicated, these probabilities associated with systems requiring the correct replies to be equal to or greater than some percentage of m. Calculations are made by use of equation 2. In a practical system with replies being displayed on a conventional PPI, the number of interrogations during one sweep of the antenna past the target will be about twenty. It will be difficult to observe random reply failures until they become a considerable percentage of the total replies to be expected. Thus, for such conditions the curves demonstrate the necessity for several reply codes if a low probability of deception is to be obtained.

ELECTRONIC INTEGRATION

If there is no integration of replies to form the friendly response, that is, if only a single correct reply is required in any beam sweep to effect a friendly recognition, the probability of deception can be made sufficiently low only by providing a large number of reply codes. This is shown by Figure 2, in which the probability of deception, P_d, given by $P_m \geq (1) = 1 - P_m(0)$, is plotted against m, the number of interrogations per beam sweep, for various values of r (the number of reply codes). As an example, if the beamwidths are limited so that there are ten or less interrogations per sweep, a probability of deception of one in a thousand could be realized with 10,000 reply codes. On the other

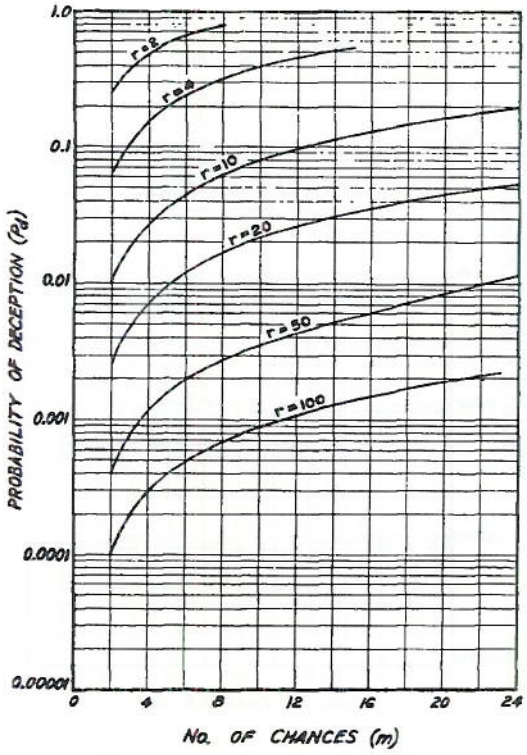


Fig. 3 - Probability of deception (P_d) for a system which requires that correct replies be received to at least two successive interrogations out of m chances. No. of reply codes = r.

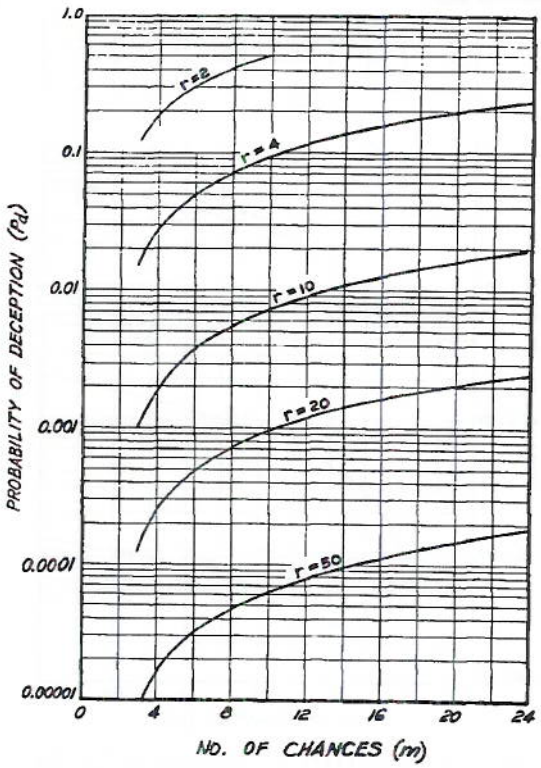


Fig. 4 - Probability of deception (P_d) for a system which requires that correct replies be received to at least three successive interrogations out of m chances. No. of reply codes = r.

hand, if a friendly response is indicated only after some integration of correct replies has taken place, fewer reply codes would be required to realize a corresponding probability of deception.

Although the necessary condition to produce a friendly indication might be the same as just discussed for direct presentation—reception of n or more correct replies out of m chances—there are other possibilities which may result in simpler techniques. For example, the devices utilized for defruiting (elimination of unsynchronized signals) serve this purpose. These circuits can be made to block signals from passing through the system unless two correct replies are received to successive interrogations (single defruiting); unless correct replies are received to three successive interrogations (double defruiting); or, as a variation, unless at least two correct replies are received to three successive interrogations. Other similar conditions which might be chosen are obvious. A device of this sort will not only permit the attainment of a low probability of deception with a limited number of reply codes but will be required to reduce the responses fed into the system from pulses arising from noise, fruit, and enemy countermeasures.

The probability that a run of n successes will occur in m interrogations has been solved.[4] The formulas for various values of m and n are given in the Appendix. Another general method of integration is to require n or more correct replies in a series of l interrogations during the m interrogations. Formulas for such systems are also given in the Appendix.

---

[4] *See Uspensky, J. V., "Introduction to Mathematical Probability," McGraw-Hill, New York, pp. 77-84, 1937.*

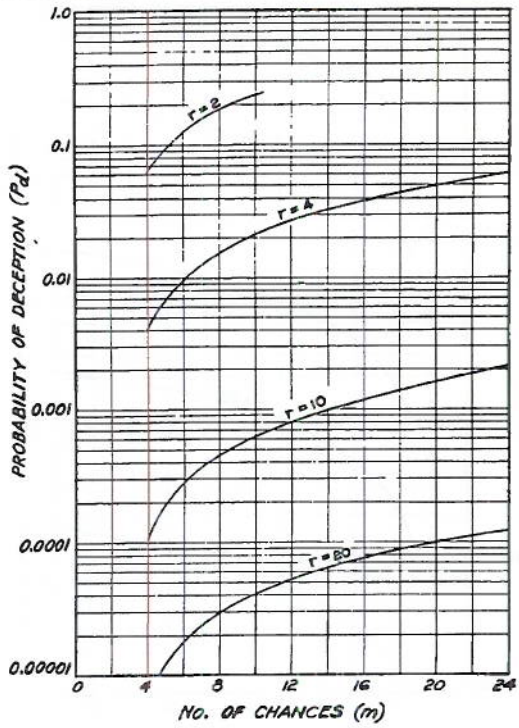


Fig. 5 - Probability of deception (P_d) for a system which requires that correct replies be received to at least four successive interrogations out of m chances. No. of reply codes = r.

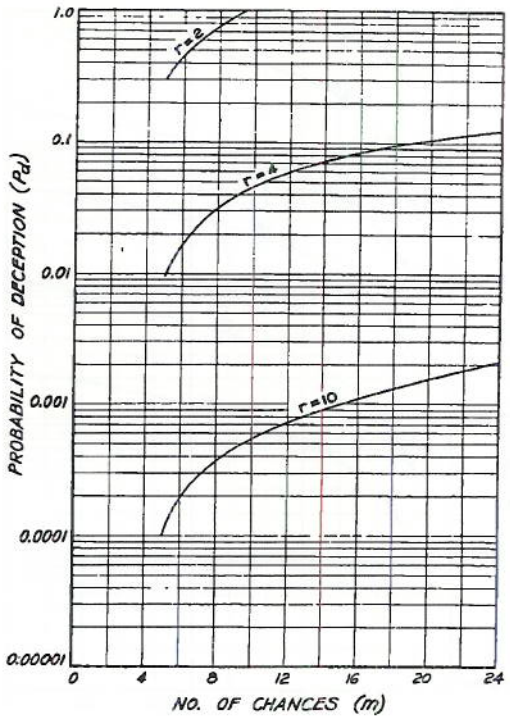


Fig. 6 - Probability of deception (P_d) for a system which requires that correct replies be received to at least five successive interrogations out of m chances. No. of reply codes = r.

PROBABILITY OF DECEPTION—RESULTS

The probability of deception (P_d) has been plotted against the number of interrogations (m) in a beam sweep, which may be expected to produce replies. Using the formulas in the Appendix, the curves are plotted for systems having the number of reply codes and method of integration as parameters. Figure 2 shows that, without some form of integration of the correct replies, a low probability of deception can be obtained only by using a very large number of reply codes. Figures 3 through 6 give the probability of deception for systems requiring two, three, four, and five correct replies to be received in succession before a friendly response is indicated. The curves for two and ten reply codes are replotted in Figure 7 to illustrate how the probability of deception is reduced by a greater amount of integration and the advantage of providing several codes.

If our own transpondors fail to reply to all interrogations in a beam sweep, a system of integration, permitting a number of failures to receive individual replies, may result in fewer failures to obtain responses. The increase in the probability of deception for such systems is illustrated in Figure 8, which is a plot for a few specific conditions.

FAILURE DUE TO TRANSPONDOR COUNT DOWN

Because a transpondor requires a finite amount of time to decode an interrogation and to reply, it may fail to respond to specific interrogations which arrive while a previous

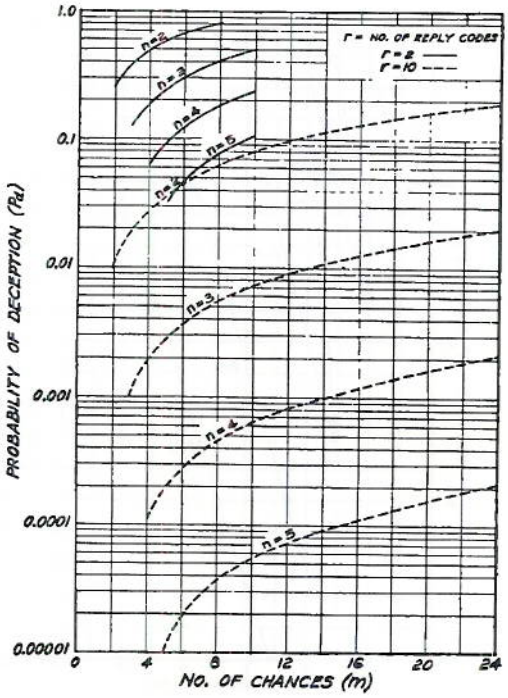


Fig. 7 - Probability of deception (P_d) for systems which require that correct replies be received to at least n successive interrogations out of m chances for the cases of the number of reply codes (r) of 2 and 10

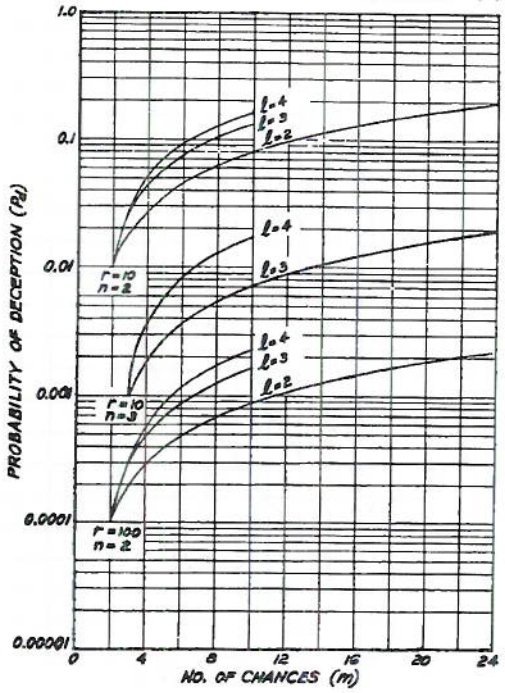


Fig. 8 - Probability of deception (P_d) for systems which require that correct replies be received to at least n out of l successive interrogations during a total of m chances. No. of reply codes = r

interrogation is being serviced. Moreover, the transpondor design may introduce an additional time beyond the reply before a new interrogation can be accepted. The time during which a transpondor is inactive because of an interrogation is referred to as the dead time. The ratio of transpondor reply signals to the interrogations received, or fractional response, is referred to as count down. A statistical treatment of transpondor count down may be found in a previous NRL report.[5]

The probability of failure, because of count down resulting from heavy traffic, to recognize one of our own transpondors can be reduced by a system design in which dead time and interrogation beams are minimized. Also, the type of reply integration may affect the probability of failure. If the arrival of interrogations at a transpondor could be considered random, the chance of failure would be quite small for any practical situation. As an example, it has been shown[6] that, for an extreme situation of 200 interrogators with an average repetition rate of 200 cps, with beamwidth of 36° and transpondor dead time of 125 microseconds, the probability of a fractional response of 56% or less is 1% or less.

---

[5] *Paull, S., "Overinterrogation and Asynchronous Replies, and Their Relation to Display Limitation and Traffic Handling Capacity in an IFF System," NRL Report R-3338, Secret, August 25, 1948.*

[6] *Paull, op. cit.*

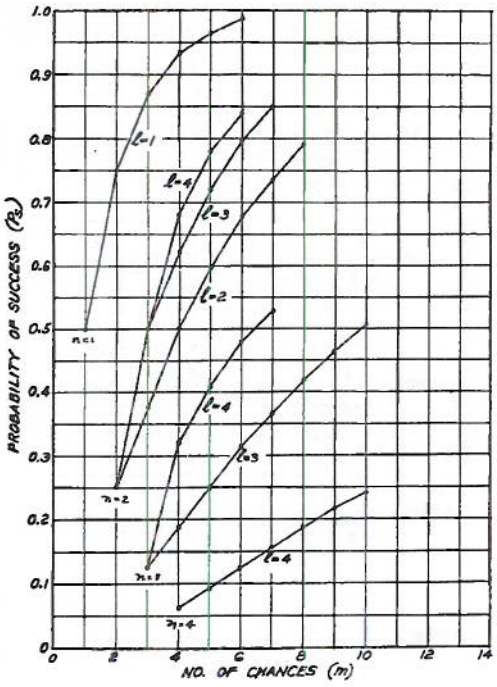


Fig. 9 - Probability of successful interrogation under conditions of 50% count down for systems requiring correct replies to be received to at least n out of l successive interrogations during a total of m chances.

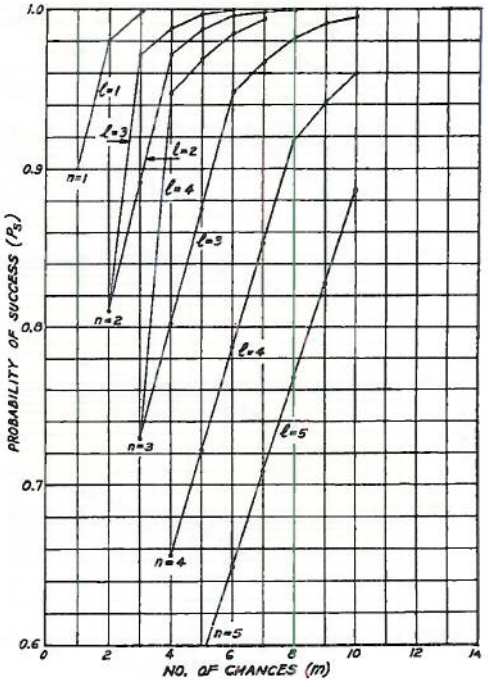


Fig. 10 - Probability of successful interrogation under conditions of 10% count down for systems requiring correct replies to be received to at least n out of l successive interrogations during a total of m chances.

Suppose now that the traffic was so great that only half of the individual interrogations produced replies during one sweep of the antenna and that the count down were random.[7] Since each reply made by a friend may be assumed correct if made at all, the probability of a correct reply being received to a single interrogation is 0.5 for these assumptions. The chances of failure to produce a friendly indication will decrease as the number of opportunities to form a friendly response increases, i.e., as m increases. Figure 9 is the probability of success plotted against m for various systems of integration for conditions of 50% count down. Figure 10 is a similar plot for 10% count down, a more reasonable figure for heavy traffic conditions.

These results are based upon the assumption that interrogations arrive at the transpondor at random. If the IFF systems collected data independently, this condition could be realized for all practical purposes. However, it has been customary to trigger the interrogator from the associated radar system, and in this situation one is limited by the radar policy with respect to the repetition rates. Under these conditions, situations may arise where the interrogations from one set will arrive during the dead time produced by another interrogator, and where the pulse repetition rates are close enough together that this situation will continue throughout the entire interrogation of the target. Thus, a condition of near synchronization could be established which would give an "instantaneous"

[7] *It should be borne in mind that, for these conditions, there is about one chance in a hundred that count down would be so high.*

[redacted]

count down so great as to cause failure regardless of the system of integration. However, over a long period of time and a large number of situations, the percentage of failures will be small and will approach a figure corresponding to the case of random interrogations.

The assumption of random interrogations is probably not too much in error for all practical situations. The factors which contribute to the relief of high "instantaneous" count down are variations in repetition rates, relative motions of the interrogators with respect to the transpondor, and differences in antenna rotation rates. In search radar systems using MTI, the repetition rate will be quite constant for a given set, although the fixed value may vary from set to set. For example, the AN/SPS-2 specification calls for a rate of 255 ± 5 per second. That is, the period may vary over an extreme range of 150 microseconds. Thus, if the transpondor could recover in 50 microseconds under low traffic conditions, in many cases the sets would become "unsynchronized" in a time corresponding to one beam sweep past the target. If complete failure were experienced during one beam sweep, very probably the two signals would be completely out of phase on the next antenna scan. When traffic conditions are high, the occurrence of dead times becomes random, and this will tend to break up the synchronized condition.

Fire control radars probably have more variable repetition frequency (up to 10%, deliberately introduced in some instances) and operate at normal rates such as 1800 or 3000 pps. Ordinarily, the IFF trigger would be counted down from these high rates. Synchronized situations for these cases would be unlikely to arise or, if they did, to exist for a time long enough to cause any trouble.

ANALYSIS AND REPLY CODES

It is obvious that the difficulty of guessing the correct reply to an interrogation increases with the number of codes. If, however, the enemy may be expected to attempt an analysis of the system through statistical examination of the reply distribution to selected interrogations, it may be advantageous to restrict the number of reply codes. That is, it may be more difficult to recognize a significant relationship if there are only a few possible replies than if there are a greater number. If this consideration is correct, two reply codes would be preferable. On the other hand, if an extremely large number of reply codes could be used so that repeats would be infrequent, a statistical examination might be defeated. Thus the eventual system design considerations must evaluate the possibilities of such a method of analysis.

THE NUMBER OF REPLY CODES REQUIRED

The actual determination of the number of reply codes required for a future IFF system will be based upon security requirements, information to be transmitted for auxiliary functions, and technical considerations. The situation may be summarized as follows:

a. The probability of an enemy guessing the correct code may be reduced by increasing the number of security reply codes from which he must make a choice.

b. Some methods of analysis employing statistical distribution of reply codes may be made more difficult either by reducing the number of reply codes used for security or by using an extremely large number.

c. The number of codes required to provide auxiliary functions can only be determined after the functions, together with the detail of intelligence required, have been

specified. On the other hand, the decision whether to incorporate an auxiliary function will be greatly influenced by what provisions can be reasonably made.

d. The greater the number of codes to be generated, for a particular method of producing them, the more complicated the equipment is likely to become.

e. If frequency-coding is used, a division of traffic may be arranged so as to reduce the number of signals on any one channel.

All things considered, it appears that an extremely large number of reply codes would not be required. A few security codes, say ten to 100, appear to be ample for a cryptographic system. If appropriate methods of integration of the replies are employed, there is very little probability of an enemy guessing the correct code. Transpondor count down is not likely to limit the form of integration chosen. For example, with 10% count down, there is a 99.5% chance of successful interrogation during an antenna sweep composed of 10 interrogations when the integration requires correct replies to be received to at least three successive interrogations. Under those conditions, the probability of deception by guessing is 0.007 for a system with ten reply codes and 0.00006 for one with 50 reply codes.

While the traffic may be reduced on any one channel by a method of frequency-coding, the expected traffic is not so great as to require more channels than necessary for the security code. Although components are not at present available for multichannel frequency-coding, there appears to be no fundamental reason why the technique is not feasible.

The auxiliary functions most likely to be associated with a future IFF system are:

a. Transpondor beacon for increasing detection range. No additional reply codes or complications are required to provide this basic function. There may, however, be a conflict between the optimum frequencies for particular beacon functions and a universal IFF.

b. Emergency signaling. At least one distinctive reply signal would be required. The important consideration is in the choice of signal type.

c. Aircraft control. Two separate requirements exist. One is for control of individual aircraft to direct them over or to a particular point in space such as for intercept. This includes the beacon function, (a) above, but in addition may require means of determining the identity of individual friendly aircraft in order to coordinate the commands with detection data. The other requirement is for control of aircraft traffic in the vicinity of a base. There is a requirement for ample reply codes to assign identities to each aircraft or unit in the approach, holding, or landing areas. Possibly 100 reply codes would be required.

d. Altitude data. Altitude data may be required as a part of the IFF system; however, the detail to be transmitted and the type of code may be determined by auxiliary functions. The most severe requirement will probably be determination of altitudes of individual planes in a stack. A minimum of ten codes will probably be required, and it might be desirable to provide 50 or more.

e. Limited communication. It may be desirable to provide facilities for making reports automatically. For example, the type or mission of aircraft may be designated by reply-coding. Acknowledgment of commands might be a requirement. The number of reply codes required is merely a function of the data to be transmitted.

[redacted]

CONCLUSIONS

In a transpondor type of IFF system, reply codes used cryptographically must not permit garbling; an enemy could generate a deliberately garbled code to appear friendly. Pulse group codes are susceptible to garbling, while frequency codes may avoid this difficulty and therefore appear to be the better choice for the security coding function.

Some auxiliary functions which the IFF system performs may, however, be accomplished by pulse reply codes. If, by chance, garbling does happen to occur, the effect would delay or reduce the efficiency of the data supplied and therefore would not have the serious consequences involved in a loss of security. One function, that of supplying altitude of individual planes in a stack by coding, may, however, be seriously impaired by persistent garbling.

Security against enemy deception by guessing the reply in a cryptographically coded system may be attained with a small number of reply codes if there is ample integration of replies before a friendly indication is recognized. Without integration, at least several thousand reply codes would be required.

Transpondor count down is unlikely to be a factor in the choice of reply-coding or integration methods.

* * *

[redacted]

[redacted]

APPENDIX

Formulas for the Probability of Deception

The formulas used for computing the probability of deception are listed here to facilitate extension, if desired, of the curves presented in this report. In all cases, p is the probability of guessing the correct reply code for a single interrogation. It is equal to the reciprocal of the number of reply codes for the type of system considered in this report. The probability of guessing incorrectly is q = 1-p. The number of continuous interrogations given, in a single beam sweep, to a target from which replies may be expected is denoted by m.

The probability that a run of at least n consecutive correct answers will be guessed in m chances when the guesses are independent and have an individual probability p of being correct is known as the "problem of runs."[8] Let the probability of a run of n in m trials be P_m and in m+1 trials P_{m+1}, etc. The difference equation,

$$P_{m+1} = P_m + (1-P_{m-n})\, p^n q, \tag{3}$$

together with the initial conditions,

$$P_0 = P_1 = \ldots. P_{n-1} = 0 \text{ and } P_n = p^n ,$$

allows P_m to be determined for m = n + 1, n + 2, etc. Thus, when m = n, equation 3 gives

$$\begin{aligned} P_{n+1} &= p^n + (1-P_0)\, p^n q \\ &= p^n + p^n q, \end{aligned}$$

since $P_0 = 0$.

When m = n+1,

$$\begin{aligned} P_{n+2} &= P_{n+1} + (1-P_1)\, p^n q , \\ &= p^n + [(1-P_0) + (1-P_1)]\, p^n q \\ &= p^n + 2\, p^n q, \text{ etc.} \end{aligned}$$

The general solution of equation 3 is[9]

$$P_m = 1 - \beta_{m,n} + p^n \beta_{m-n,\, n},$$

---

[8] *For a detailed treatment, see Uspensky, loc. cit.*

[9] *Uspensky, loc. cit.*

[redacted]

where

$$\beta_{m,n} = \sum_{j=0}^{\frac{m}{n+1}} (-1)^j \, C_j^{m-jn} \, (p^n q)^j$$

$$\beta_{m-n,n} = \sum_{j=0}^{\frac{m-n}{n+1}} (-1)^j \, C_j^{m-n-jn} \, (p^n q)^j \, .$$

By use of the step-by-step method, or the general solution, the following group of formulas are derived in the form for convenient computation for any value of p and specific values of m and n.

n	m	
2	2	p^2
	3	$2p^2 - p^3$
	4	$3p^2 - 2p^3$
	5	$4p^2 - 3p^3 - p^4 + p^5$
	6	$5p^2 - 4p^3 - 3p^4 + 4p^5 - p^6$
	7	$6p^2 - 5p^3 - 6p^4 + 9p^5 - 3p^6$
	8	$7p^2 - 6p^3 - 10p^4 + 16p^5 - 5p^5 - 2p^7 + p^8$
	9	$8p^2 - 7p^3 - 15p^4 + 25p^5 - 6p^6 - 9p^7 + 6p^8 - p^9$
	10	$9p^2 - 8p^3 - 21p^4 + 36p^5 - 5p^6 - 24p^7 + 18p^8 - 4p^9$
	15	$14p^2 - 13p^3 - 66p^4 + 121p^5 +$ terms in higher powers of p
	20	$19p^2 - 18p^3 - 136p^4 + 256p^5 + 1791p^6 +$ terms in higher powers of p

n	m	
3	3	p^3
	4	$2p^3 - p^4$
	5	$3p^3 - 2p^4$
	6	$4p^3 - 3p^4$
	7	$5p^3 - 4p^4 - p^6 + p^7$
	8	$6p^3 - 5p^4 - 3p^6 + 4p^7 - p^8$

	9	$7p^3 - 6p^4 - 6p^6 + 9p^7 - 3p^8$
	10	$8p^3 - 7p^4 - 10p^6 + 16p^7 - 6p^8$
	15	$13p^3 - 12p^4 - 45p^6 + 81p^7 +$ terms in higher powers of p
	20	$18p^3 - 17p^4 - 105p^6 + 196p^7 +$ terms in higher powers of p
4	4	p^4
	5	$2p^4 - p^5$
	6	$3p^4 - 2p^5$
	7	$4p^4 - 3p^5$
	8	$5p^4 - 4p^5$
	9	$6p^4 - 5p^5 - p^8 + p^9$
	10	$7p^4 - 6p^5 - 3p^8 + 4p^9 - p^{10}$
	15	$12p^4 - 11p^5 - 28p^8 + 49p^9 - 21p^{10} +$ terms in higher powers of p
	20	$17p^4 - 16p^5 - 78p^8 + 144p^9 - 66p^{10} +$ terms in higher powers of p
n	m	
5	5	p^5
	6	$2p^5 - p^6$
	7	$3p^5 - 2p^6$
	8	$4p^5 - 3p^6$
	9	$5p^5 - 4p^6$
	10	$6p^5 - 5p^6$
	15	$11p^5 - 10p^6 - 15p^{10} + 25p^{11} - 10p^{12}$
	20	$16p^5 - 15p^6 - 55p^{10} + 100p^{11} - 45p^{12} +$ terms in higher powers of p

The formulas for computing the probability of guessing n correct replies in l successive chances out of a series of m interrogations may be derived by a step-by-step process from a difference equation. As before,

$P_{m+1} = P_m +$ the probability that a success occurs only because of the event, m+1.

The second term in the equation will be the probability that a combination will be formed in which (1) event m+1 is a success, (2) event m+1 is preceded by one of the C_{n-1}^{l-1} combinations of n-1 correct events and l-n incorrect events, (3) event m-n is incorrect, and (4) events prior to event m-n are such that no success has been attained by event m. This latter condition offers some difficulty. It is found convenient to divide the second term in the equation into two parts. The first part is general and is

$$C_{n-1}^{l-1} \left[1 - P_{m - 2l+n}\right] p^n (1+p)^{2(l-n)+1} .$$

This term gives the probability that a success has not occurred by event m - $2l$+n and that a success occurs only because event m+1 is correct when only n events are correct beyond event m - $2l$+n. The second part consists of the probability associated with those arrangements which permit one or more correct guesses in the events m - $2l$+n+1 to m-l. When m is small, these can be easily enumerated. This term will be denoted by P_e. Thus, the complete difference equation is

$$P_{m+1} = P_m + C_{n-1}^{l-1} \left[1 - P_{m-2l+n}\right] p^n (1-p)^{2(l-n)+1} + P_e . \qquad (4)$$

The initial conditions are

$$P_0 = P_1 = \ldots . + P_{n-1} = 0; \; P_n = p^n .$$

The lowest power of p in the final formula will be n, while the lowest power of p in P_e will be n+1. Further, its coefficient will be small. Thus, when p is small, an approximation satisfactory for most purposes may be had by neglecting P_e.

Formulas for computing the probability of deception for some specific values of n and l plotted are:

n	l	m	P_d
2	3	2	p^2
		3	$3p^2 - 2p^3$
		4	$5p^2 - 6p^3 + 2p^4$
		5	$7p^2 - 11p^3 + 6p^4 - p^5$
		6	$9p^2 - 16p^3 + 9p^4 - p^6$
		7	$11p^2 - 21p^3 + 9p^4 + 10p^5 - 11p^6 + 3p^7$
		8	$13p^2 - 26p^3 + 5p^4$ approx. for small values of p
		9	$15p^2 - 31p^3$ approx. for small values of p
		10	$17p^2 - 36p^3$ approx. for small values of p

2	4	2	p^2
		3	$3p^2 - 2p^3$
		4	$6p^2 - 8p^3 + 3p^4$
		5	$9p^2 - 17p^3 + 12p^4 - 3p^5$
		6	$12p^2 - 28p^3 + 27p^4 - 12p^5 + 2p^6$
		7	$15p^2 - 41p^3$ approx. for small values of p
		8	$18p^2 - 54p^3$ approx. for small values of p
		9	$21p^2 - 67p^3$ approx. for small values of p
		10	$24p^2 - 80p^3$ approx. for small values of p

n	l'	m	P_d
3	4	3	p^3
		4	$4p^3 - 3p^4$
		5	$7p^3 - 9p^4 + 3p^5$
		6	$10p^3 - 16p^4 + 8p^5 - p^6$
		7	$13p^3 - 23p^4 + 12p^5 - p^7$
		8	$16p^3 - 30p^4$ approx. for small values of p
		9	$19p^3 - 37p^4$ approx. for small values of p
		10	$22p^3 - 44p^4$ approx. for small values of p

There is an alternative method of calculating the probability of deception which is useful if formulas are not available for the method of integration used. The probability of obtaining a combination which will give a friendly indication is computed separately for each group of combinations containing n correct replies in the m chances. The probability of deception will be the sum of the terms found by letting n vary from zero to m. Now if p is small, the chances of guessing an appreciable number of correct replies in a limited number of chances is small. Thus in this case a good approximation is found by using only a few terms starting with n = 0. The maximum error in such an approximation may be determined by computing $1 - P_m(\geq n)$, where n is the largest number of correct replies in m chances considered.

* * *

[redacted]