SG1I

[redacted]

Using table 4 and the .80 probability of being correct that they cite on page 11, they following can be stated.

There are 32 possible 5-bit permeations for generated outputs. All 32 can be grouped with into a 0, 1, or 2 error message box with a .94208 reliability. (Some of the permeationstions fit into both 1 and 2 error boxes, and all of the 2 error entries ~~are redundant~~ match to both the (00000 and the 11011) or the (01110, and 10101) correct messages. That is, 2 error messages do not (as P&T suggest) uniquely identify a correct message, but only narrow the likely choices to 2.

Because of the 4 correct message codes they chose, several things happen. If a "correct" message is received, (eg. 00000) then it must be remembered that it also could be a 3 error message of 01110 or 10101, or a 4 error message of 11011. Since a 0 error message (p = .32768) is roughly 6 times as likely as a 3 error message (~~p =~~ .0512) ~~and~~ 50 times as likely as a 4 error message (.0064) then the 00000 choice is at least 6 times (p ≃ .82) more likely than each of the other choices, but is only about 3 times (p = .67) [.0512 + .0512 + .0064 = .1088] more likely ~~than~~ all of the other messages. Most of the ~~or~~ 1 error messages have even smaller odds of ~~correlating to their~~ ~~specific~~ uniquely identifying a specific correct message. For instance, the receipt of 00100 is (as shown in Table 4) a one error message of 00000. However, (not shown in Table 4) it also is a 2 error message of both 01110 and 10101. Since the odds of a two error message ~~are~~ p = .2048 and there are two possibilities, the message 00100 gives only ~~p~~ an ≃ .5 chance of the message 00000 being correct (p = .4096) relative to p = .4096 for (.2048 + .2048 (being either 01110 or 10101)

The statistics get hairy here, and I haven't tried to do them fully, but the curve for "no error correcting" is very wrong (see inserted green curve ~~for~~ on Table 4) and I would bet that the "error correcting" curve is also erroneously high. Hence, I am suspicious of the accuracy of the "majority vote" curve.

[redacted] SG1I

Approved For Release 2000/08/07 : CIA-RDP96-00787R000500070003-9

00000
01110
10101
11011

$P_4(00000) = .00128$
$P_1(01110) = .08192$
$P_3(10101) = .00512$
$P_2(11011) = .02048$

$P_c \cong .75$
$\Sigma = .02688$
$\sim 3:9$

0 1 1 1 1

$P_0 = (.8)^5 = .32768$

$P_1 = (.8)^4(.2) = .08192$

$P_2 = (.8)^3(.2)^2 = .02048$

$P_3 = (.8)^2(.2)^3 = .00512$

$P_4 = (.8)^1(.2)^4 = .00128$

$P_5 \quad (.2)^5 = .00036$

0 1 1 0 1

$P_3 \; (00000) = .00512 \quad (12.5\%)$
$P_2 \; (01110) = .02048 \quad (37.5\%)$
$P_2 \; (10101) = \quad (37.5\%)$
$P_3 \; (11011) = \quad (12.5\%)$