[redacted]

NRL REPORT NO. R-3102

[redacted]

[redacted]

INTERIM REPORT

ON

NRL DEVELOPED SPR CODE GENERATORS

★

FR-3102

[redacted]

[redacted]

NAVAL RESEARCH LABORATORY

Washington, D.C.

NRL REPORT NO. R-3102

DECLASSIFIED

INTERIM REPORT
ON
NRL DEVELOPED SPR CODE GENERATORS

by

Bert Fisk and C. L. Spencer

June 1947

Problem No. S1398

Approved by:

L. A. Gebhard
Superintendent
Radio Division II

Commodore H.A. Schade, USN
Director
Naval Research Laboratory

NAVAL RESEARCH LABORATORY
Washington, D.C.

DECLASSIFIED

DISTRIBUTION

	Copy No.
BuShips	
925A	1 - 10
ONR	
(N-482)	11 - 14
JRDB	
Attn: Library	15 - 16
Attn: Navy Secretary	17

CONTENTS

ABSTRACT

The code generator described in this report was designed and built at the Naval Research Laboratory for use with engineering models of the SFR facsimile security system. It is capable of producing mark-space cipher at the synchronous rates of 1000, 666-2/3, and 333-1/3 cipher units per second as desired. It delivers a random type cipher that averages fifty percent mark and fifty percent space, and is of such a nature as to cover thoroughly and completely any transmitted facsimile copy against visual attack. The cipher cycle is of such length that continuous operation for long periods of time is feasible. The design for an improved model that would be better able to withstand compromise is also included.

REFERENCES

1. NRL Report R-3015, 19 November 1946: Interim Report on Experimental Synchronous Polarity Reversal Equipment.

Original Data recorded in NRL Log Book 6182.

INTERIM REPORT ON NRL DEVELOPED SPR CODE GENERATORS

INTRODUCTION

1. The problem of designing and building SPR equipment for Naval test purposes was initially divided into two parts. The design of the electronic part of the equipment was assigned to NRL, while the development of a suitable code generator was assigned to the Naval Computing Machine Laboratory. Unavoidable delays and difficulties encountered in design delayed delivery of the code generators so that NRL designed and built the interim code generator described in this report in order to be able to proceed with circuit tests of the equipment as a whole. Further improvements providing a higher degree of security for this device, even in the event of compromise, are also included for whatever they may be worth.

2. The type of code needed to operate properly with the SPR system is that of a random mark-space character, the mark output being a negative 50 volts and the space output zero volts. Additional requirements are: The generator must be capable of delivering its output at synchronous speeds of 1000, 666-2/3, and 333-1/3 cipher elements per second; it must be possible to achieve synchronism between two machines in a reasonable length of time; the cipher produced must average very close to "half and half" to give satisfactory coverage of transmitted material.

3. The present experimental NRL SPR code generator employs five continuously-rotating code disks scanned photoelectrically. The disks have respectively 95, 97, 99, 101, and 103 code elements each, and are driven in such a way that one thousand elements per second are scanned on each disk. The code elements in each disk consist of holes cut in the disk, through which a beam of light can pass from an exciter lamp to a photoelectric cell. A key is produced on each disk by randomly covering approximately one half of these holes, so that as the disk turns, light will activate the photoelectric cell only as the open holes pass the light beam. The five code disks are mechanically adjusted in such a way that five code elements (one on each disk) are scanned simultaneously, that is, one code element on each of the five disks is scanned every one-thousandth of a second. The five outputs from the photoelectric cells are combined electronically in special cancellation-type circuits in such a way that if for any one-thousandth of a second, none, any two, or any four of the photoelectric cells are giving an output, the code output generator will be "mark" or minus 50 volts. If any one, three, or five of the photoelectric cells give an output, the code generator output will be "space" or zero volts. Thus the output of the code generator will be the result of the binary sum of the signals from the five code disks. If a "mark" output from the equipment is chosen as 1 and a space as 0, and if an open hole in a disk is chosen as 0 and a closed hole as 1, then the above mentioned operation will resolve itself into simple binary addition, employing the assumptions that $0+0=0, 0+1=1$, and $1+1=0$.

4. A block diagram of the equipment is shown in Figure 1. In this device no input to a cancellation circuit gives no output; one input, only, gives an output; two simultaneous inputs to a cancel-

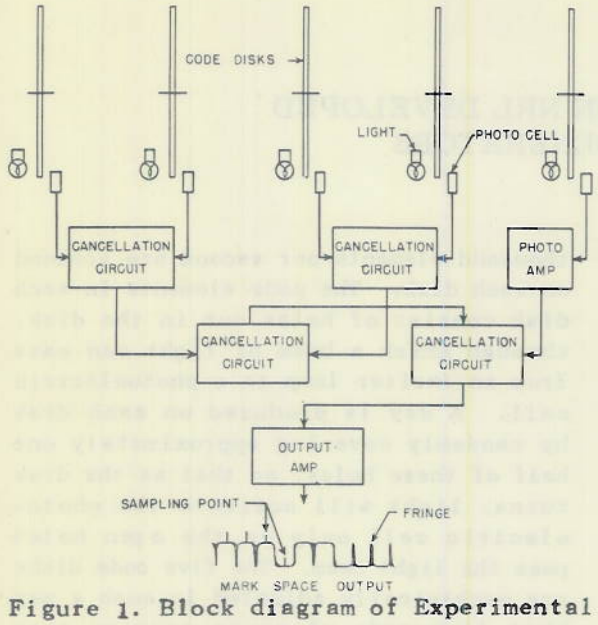


Figure 1. Block diagram of Experimental NRL Code Generator

lation circuit cancel each other and give a net of no output to the next circuit. The output amplifier gives mark output with no input and space output when it receives an input.

5. An especially designed clutch which permits a synchronous start of the code disks from preset stationary positions is used to start the code machines in operation without getting the synchronous drive motors out of step. This clutch is tripped electrically by a circuit that permits the teeth of the clutch to engage in approximately eight milliseconds after the occurrence of an initiating pulse. Since both transmitting and receiving machines are tripped automatically, their start is practically simultaneous and therefore the two machines will be started within a very few milliseconds of each other, thus making it possible to exactly phase the receiving machine to the transmitting machine in a very short time by means of the continuous phase-shifter in the receiving SPR.

6. This code machine produces a random-type code cycle of one hundred nine days length when delivering code at one thousand bauds per second, and proportionally longer for each of the slower speeds. The code disks may be set to start at any point in this long cycle. Different cycles may be selected by rearranging the open and closed holes in each of the code disks. Present analyses indicate that the cipher produced by this generator would be extremely tedious but not impossible to break as long as the details of the machine are not compromised. An improved model that can withstand compromise can be built without any increase in size or added difficulty in operation.

CODE DISK DESIGN

7. The experimental model of the NRL code generator uses five continuously rotating code disks that are made of 1/32-inch aluminum alloy and average about four inches in diameter. Forty-eight-pitch gear teeth are cut around their peripheries and the code disks are arranged about a single drive gear in such a way that they all mesh with it simultaneously as shown in Figure 2. The

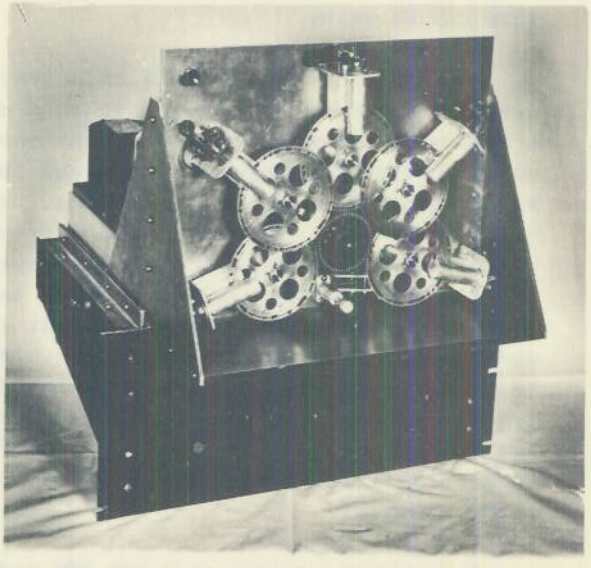


Figure 2. Front View - Experimental Code Generator

disks have respectively 206, 202, 198 194, and 190 teeth each, and the driving gear has 120 teeth. Since there is one code element on each disk for each two

teeth, each code disk will produce the same number of code elements per second. The code elements of each disk consist of 0.081-inch square holes cut in the disk 1/8 inch from the circumference. A key is produced on each disk by randomly covering approximately one half of these holes with black masking tape. All the holes in a disk are consecutively numbered from one up to the total number of holes in each disk, so that it is possible to preset the code machines prior to a synchronized start.

8. Each disk is fitted with an oilite-bronze center bearing, and is supported on the end of a post by means of a machined, knurled thumb screw which can be unscrewed to remove the disk. The posts are mounted in slots and are provided with tension springs and stops so that each disk may be disengaged from the driving gear and turned to any desired position for an initial set-up and then re-engaged by sliding the post back into place.

SCANNING MECHANISM

9. The code disks are scanned by shining a beam of light from a projection lamp through a 0.061-inch wide oblong hole in the lamp enclosure, through the holes in a disk as it rotates, and then through another 0.061-inch oblong hole in a light-tight shield can that contains a Type 927 gas photoelectric tube. In the present model, these scanning "heads" are located on the opposite side of the code disks from the drive gear. The design and location of these parts is shown in Figure 2. When the light beam is interrupted by the code disk the photoelectric tubes give zero output; the presence of the beam gives negative 12 to 15 volts.

CANCELLATION - COMBINATION CIRCUITS

10. The outputs from the five photoelectric scanners are combined binarily in such a way that for a particular baud of cipher, the output from the machine will be "mark" if the holes in all five disks at that instant are closed, or if any two or four are open. The output will be "space" if any one or three or all five holes are simultaneously open. This binary addition is accomplished by combining pairs of outputs from the photo tubes in special cancellation circuits. The outputs from the paired circuits are fed into other cancellation circuits two at a time until all five photo tubes are accounted for. This process is illustrated in Figure 1.

11. Figure 3 is the fundamental diagram of the cancellation circuits. Tubes

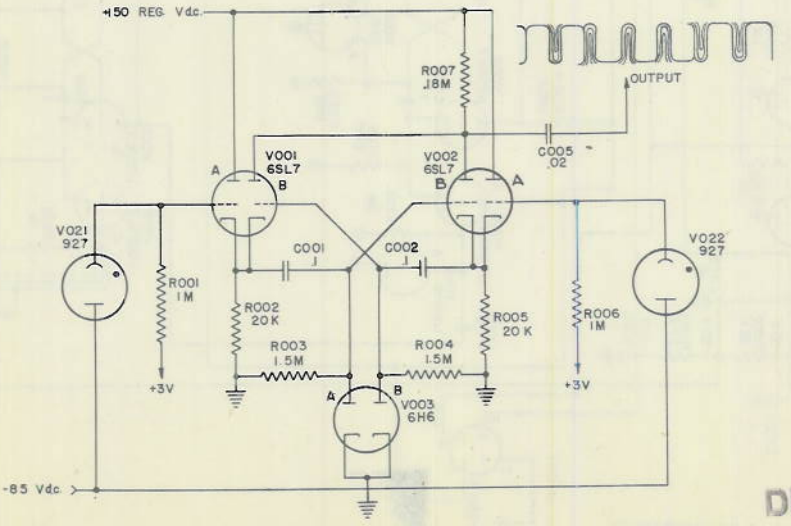


Figure 3. Cancellation-Combination circuit

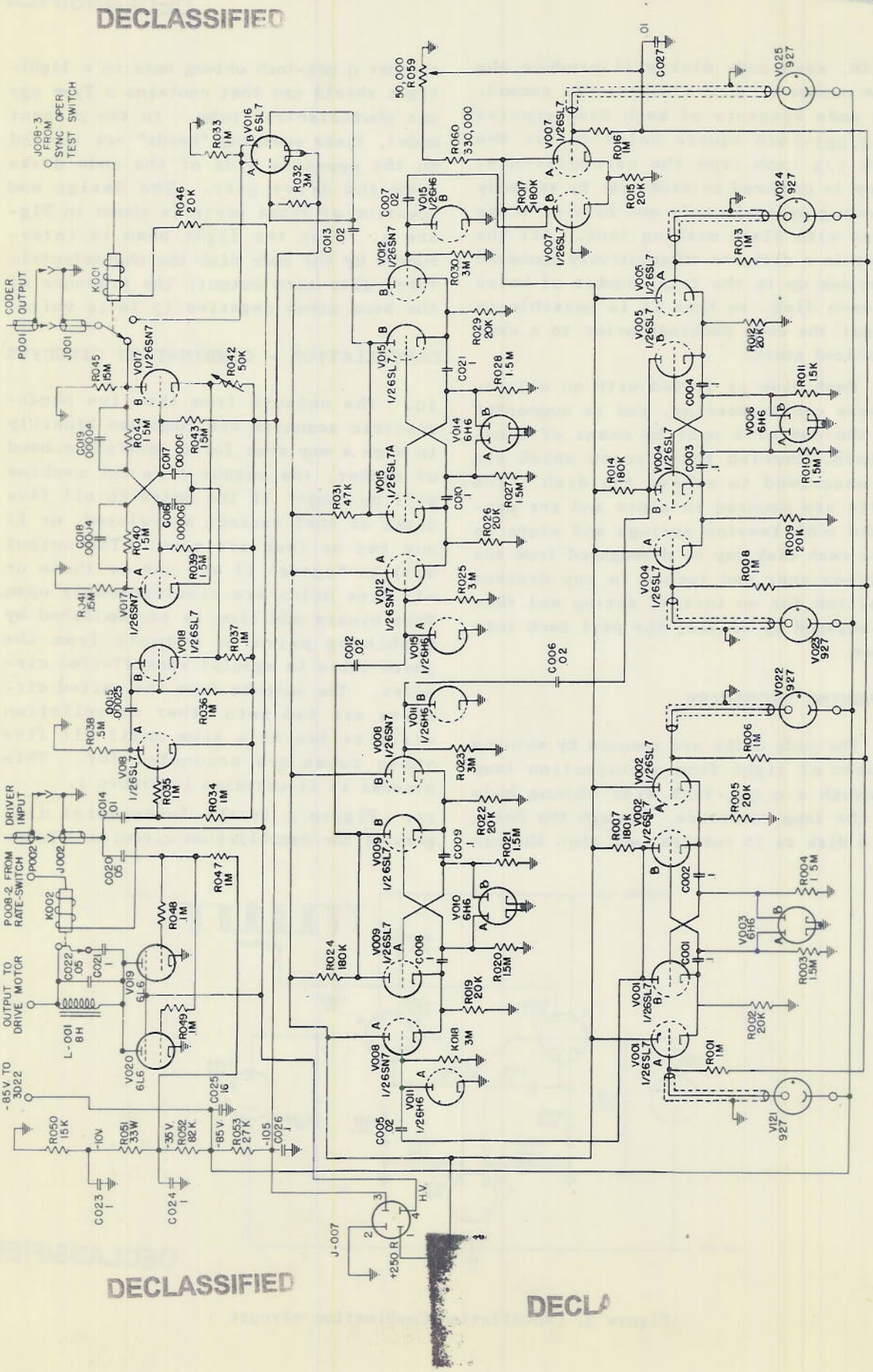


Figure 4. Schematic diagram of Experimental Code Generator

V-001-B and V-002-B are normally biased at cutoff by the current drawn through R-002 and R-005, respectively by V-001-A and V-002-A. If a beam of light enters the phototube V-021, the tube will conduct, and the grid of V-001-A will go negative beyond cutoff, thus driving the connected cathodes negative, making V-001-B conduct, and thereby giving a negative swing at the plate output of the circuit. The grid of V-002-B is also coupled to the cathode of V-001-A and will swing negative with it, but since V-002-B is already at cutoff, nothing additional will happen as a result of this negative excursion. If both phototubes V-021 and V-022 receive simultaneous beams of light, then the cathodes of both V-001 and V-002 will go negative, but since the grid of each is cross connected to the cathode of the other, neither V-001-B nor V-002-B will conduct and consequently there will be no output. The reason is that the grid and cathode of each tube have gone negative by the same amount, and neither tube will conduct. Thus cancellation occurs when the circuit receives two simultaneous inputs. The diode V-003 serves as a d-c restorer to maintain a definite voltage limit on the grids of V-001-B and V-002-B. This is the fundamental operation of all the cancellation circuits used in this device as illustrated in Figures 1, 4, and 5. The 6H6 diodes function as d-c restorers on all grids that have condenser inputs.

CLUTCH MECHANISM FOR INSTANTANEOUS SYNCHRONOUS START

12. To transmit a message by the SPR system the code generators at the transmitting and receiving stations must be in exact step. If the code machines are as much as one baud out of step, only a garble will be received. Therefore, it is essential that the code disks in both code machines be preset to exactly the same setting and then started at exactly the same instant. This is accomplished in the NRL code generator by means of an especially designed clutch that is tripped electrically in both the transmitting and receiving SPRs by the operation of a single switch at the transmitting apparatus. If there are a few bauds difference in the two codes after the initial start, the receiver operator can correct phase to get into step by means of the continuous phase shifter in the SPR.

13. The design of this clutch is shown in Figures 6, 7, and 8. The clutch is

Figure 5. Bottom View of Code Generator

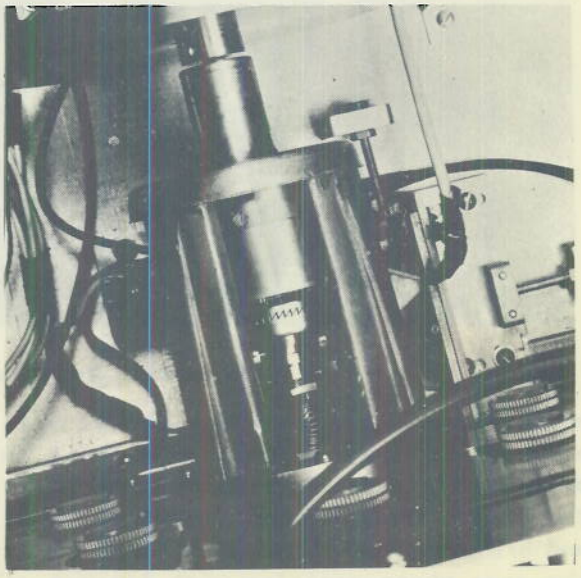


Figure 6. Top View of Clutch

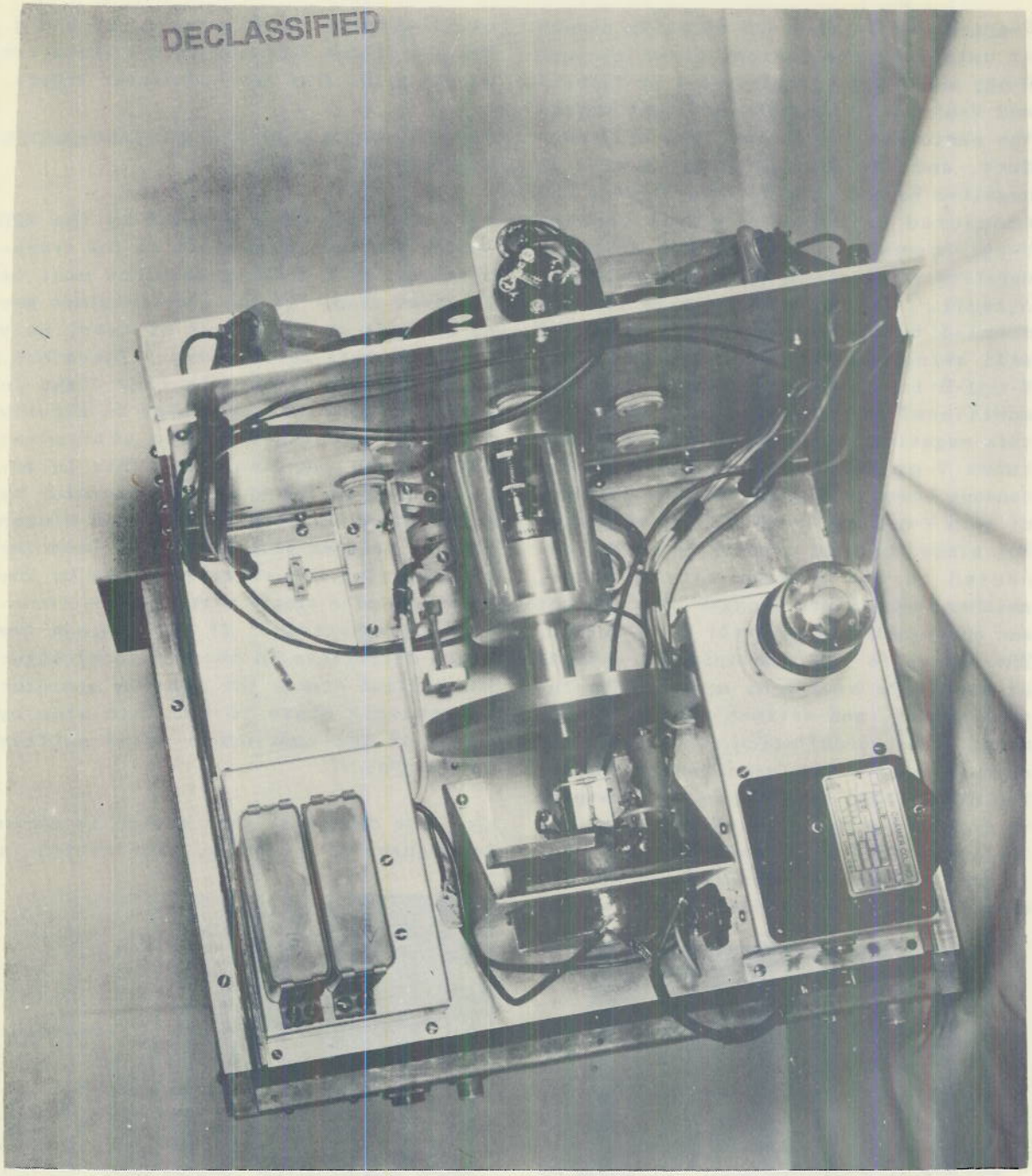
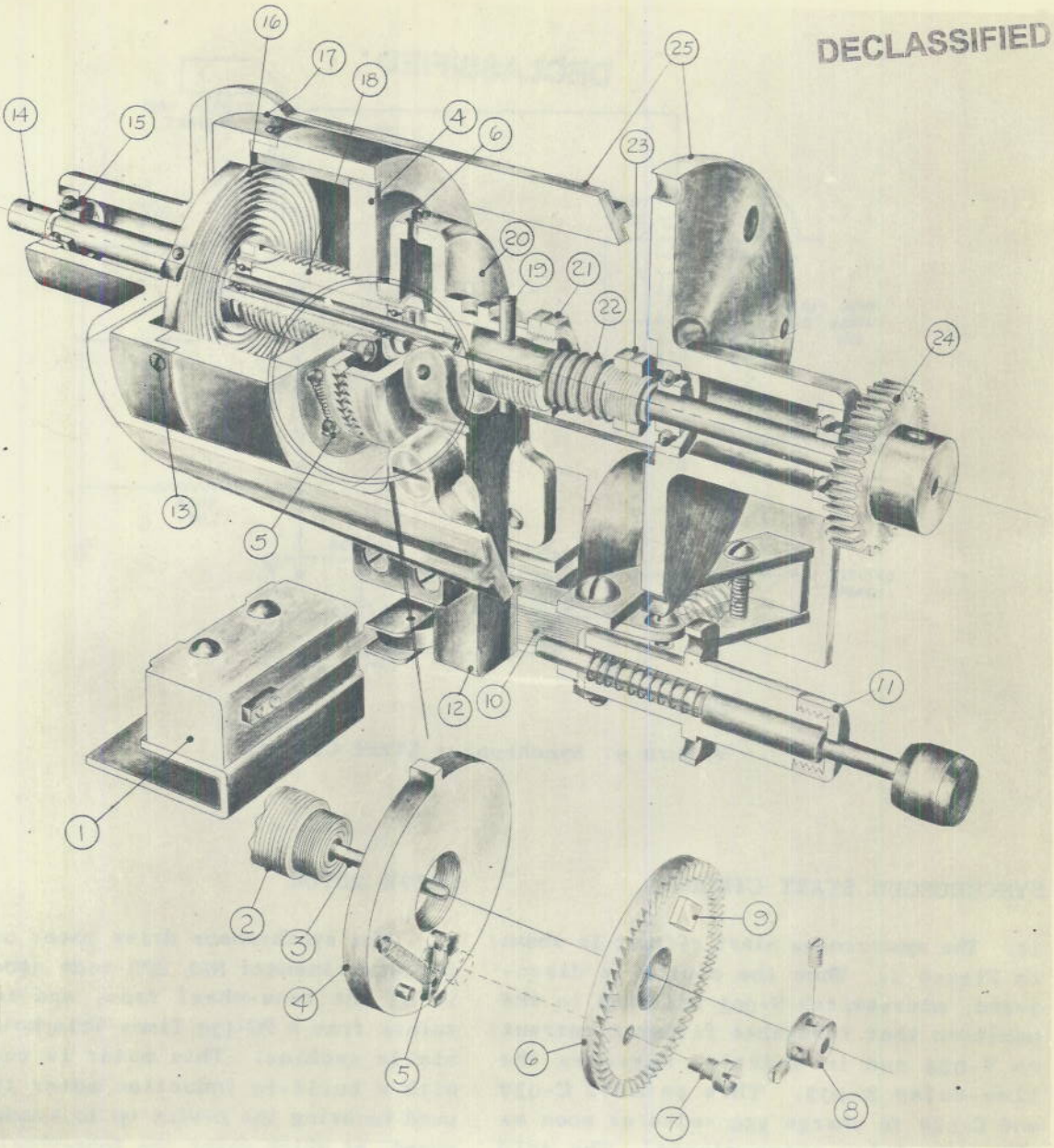


Figure 7. Top View of Code Generator

spring-loaded in such a way that it will wind up as many as 20 revolutions in bringing the code disks up to speed after the clutch teeth engage, and then unwind and bring the code disks back into exactly the same phase position with respect to the driving motor as at the instant the clutch engaged. This action enables the code disks to be started from a standing, preset position and be brought up to synchronous speed and into exact phase with the drive motor without overloading the motor and causing it to drop out of phase and stop.



1. Micro-switch
2. Threaded driving plate shaft
3. and 14. Drive shaft
4. Stop plate
5. Spring loaded stop
6. Buttressed toothed driving plate
7. Driving plate stop screw
8. Drive shaft retaining collar
9. Counter weight
10. Clutch tripping magnet
11. Clutch throw - out plunger
12. Clutch throw - out yoke and arm
13. Clutch spring tension adjustment screws
14. same as three
15. Drive shaft support bearings
16. Clutch spring
17. Clutch spring housing
18. same as two
19. Driven plate retaining pin
20. Buttressed toothed driven plate
21. Driven plate retaining pin spacing nuts
22. Driven plate engaging spring
23. Driven plate engaging spring tension adjustment nuts
24. Code disks driving gear
25. Clutch frame

Figure 8. Cutaway View of Clutch Mechanism

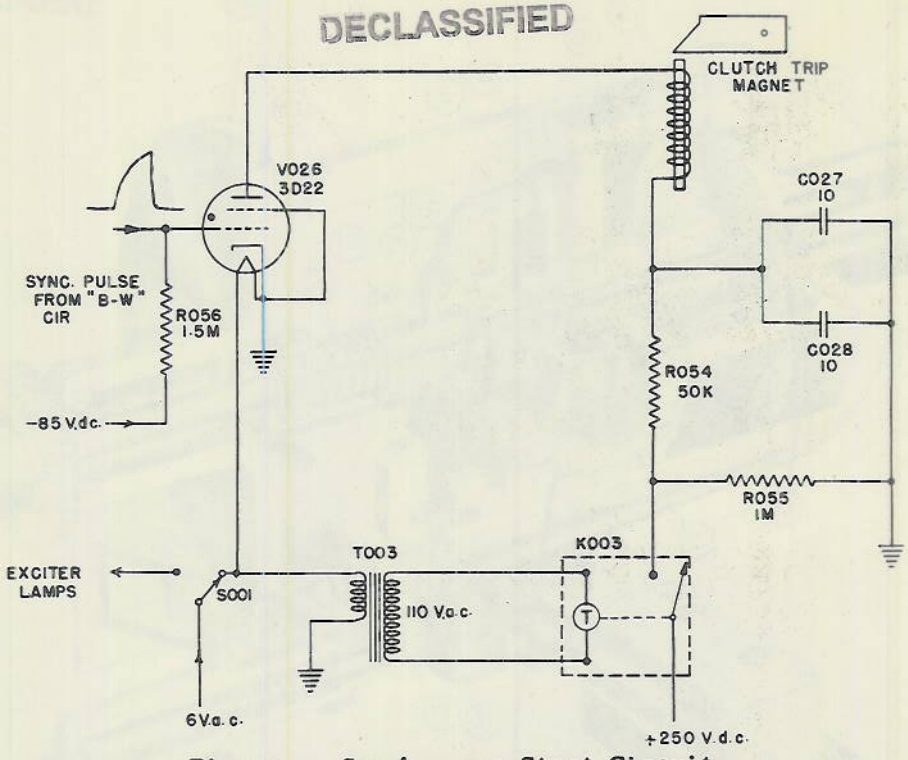


Figure 9. Synchronous Start Circuit

SYNCHRONOUS START CIRCUIT

14. The synchronous start circuit is shown in Figure 9. When the clutch is disengaged, microswitch S-001 switches to the position that furnishes filament current to V-026 and in addition operates the time-delay K-003. This permits C-027 and C-028 to charge 250 volts as soon as the time-delay relay closes. The grid of thyratron V-026 is biased at negative 85 volts, and therefore the tube will not fire until the large positive sync pulse is received from the SPR. When the sync pulse fires V-026, thus discharging C-027 and C-028 through the clutch trip magnet K-004, the clutch engages and the microswitch is switched to the position to light the exciter lamps. This tripping action requires approximately one millisecond from the time the tube fires until the clutch teeth engage. Location of the parts of this circuit are shown in Figures 6, 7, and 8.

DRIVE MOTOR

15. The synchronous drive motor used in the experimental NRL SPR code generator is of the tone-wheel type, and was obtained from a RC-120 Times-Telephoto facsimile machine. This motor is equipped with a built-in induction motor that is used to bring the device up to synchronous speed, at which point the tone-wheel takes over and maintains synchronous drive. The design of this motor is such that the shaft revolutions per minute is the same as the driving frequency in cycles per second; that is, if 1000 cycles per second is used as the driving frequency, the motor will turn 1000 revolutions per minute. The motor was modified in such a manner that the two sets of field coils are connected in parallel rather than in series as in the original design, thus giving a little additional power output. As measured by a prony brake, the maximum available torque which this motor can

produce is eight ounce-inches, which is borderline for the operation of this type of machine. However, it was the only motor available that could be made to operate directly from the control frequencies available, that is, 1000, 666-2/3, and 333-1/3 cycles per second. In order to prevent the motor from getting out of step and consequently stopping when the clutch was engaged during the synchronous start of the machines, it was necessary to use a heavy flywheel to absorb the starting shock when the clutches engaged. A more powerful motor would be essential if the equipment were used for anything other than experimental purposes.

DRIVE MOTOR AMPLIFIER

16. As shown in Figure 10, two parallel-coupled 6L6 tetrodes biased at cut-off

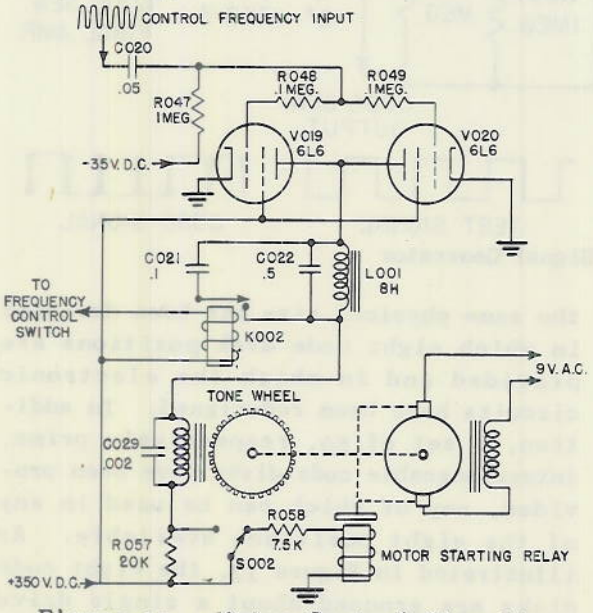


Figure 10. Motor Control Circuit

and driven directly by the SPR control frequency are used as the drive-motor amplifier tubes. Inductance L-001, and condencers C-022, and C-021 are used to couple the plates of the driver tubes to the tone-motor field so as to provide a series-resonant circuit. The motor field functions as the inductance, and C-022 and C-021 as the capacitance. Inductance L-001 functions merely as a direct-current path. This resonant circuit increases the effective voltage across the motor windings and consequently gives added power at the resonant frequency, but sharply reduced power at other frequencies. In order to maintain resonance at the three frequencies of operation--1000, 666-2/3, and 333-1/3 cycles--only C-022 is operative in the resonant circuit for 1000-cycle operation; at the two lower frequencies, C-021 is added in parallel to C-022 by the closing of K-002.

17. Since the tone motor is not self-starting, an induction-type motor built into the same frame is used to bring it up to synchronous speed. When switch S-002 is operated to the start position, the voltage to the tone motor is reduced and current is supplied to the brush closing magnet, thereby energizing the induction motor.

TEST-SIGNAL GENERATOR

18. The test-signal generator is built up in conjunction with the code generator in order that an alternate mark-space signal may be supplied to the SPR equipment and to aid in properly tuning up transmitting and receiving apparatus on a communications link. In service tests, it has been found that this test signal is essential in securing a proper setup of equipment. The SPR equipment is properly interlocked through its "sync-operate-test" switch so that no picture information can be transmitted by accident when the test signal is supplanting the random cipher.

19. V-018-A of Figure 11 is driven by the SPR control frequency and operates as an over-driven amplifier; consequently its output is a reasonably good square wave. This square wave is differentiated and rectified in diode-connected V-018-B so that the output from the cathode of V-018-B consists of positive pulses which coincide with the upward swing of the initial square wave. These positive pulses are applied simultaneously to

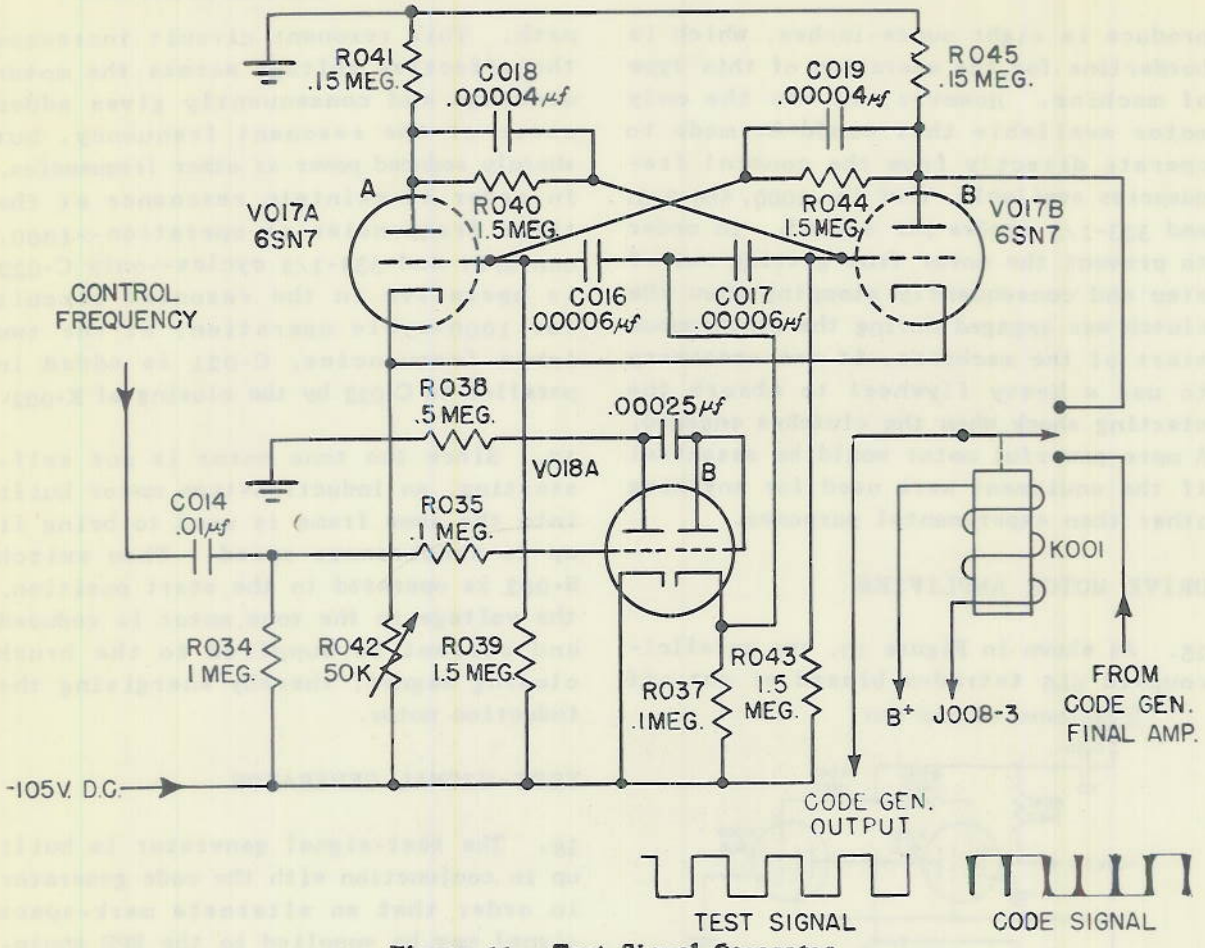


Figure 11. Test Signal Generator

the grids of the Eccles-Jordan circuit V-017-A and V-017-B, and cause it to flip alternately back and forth with each pulse received. Thus the output from the plate of V-017-B consists of a square wave that is alternately zero and negative 50 volts each cycle of the input control frequency. Relay K-001 is controlled by the "sync-operate-test" switch in the SPR, and switches the code generator output to the test signal when the switch is in the test position, and to the random cipher when the control switch is in either of the other two positions.

PROPOSED IMPROVED MODEL FOR HIGHER SECURITY

20. To alleviate the deficiencies of the present experimental NRL SPR code generator, a new model of approximately the same physical size has been designed in which eight code disk positions are provided and in which the electronic circuits have been redesigned. In addition, a set of 50, respectively prime, interchangeable code disks have been provided, any of which can be used in any of the eight positions available. As illustrated in Figure 12, the eight code disks are grouped about a single drive gear and are scanned at the point where each makes contact with the drive gear, thus eliminating the necessity of any adjustment of the scanning mechanism when code disks are interchanged. It has been found desirable to reduce the relative size of the code disks by a small amount, to construct them with one gear tooth per code element, and to equip each with double ball bearings instead of the present bronze type. The clutch mechanism and the

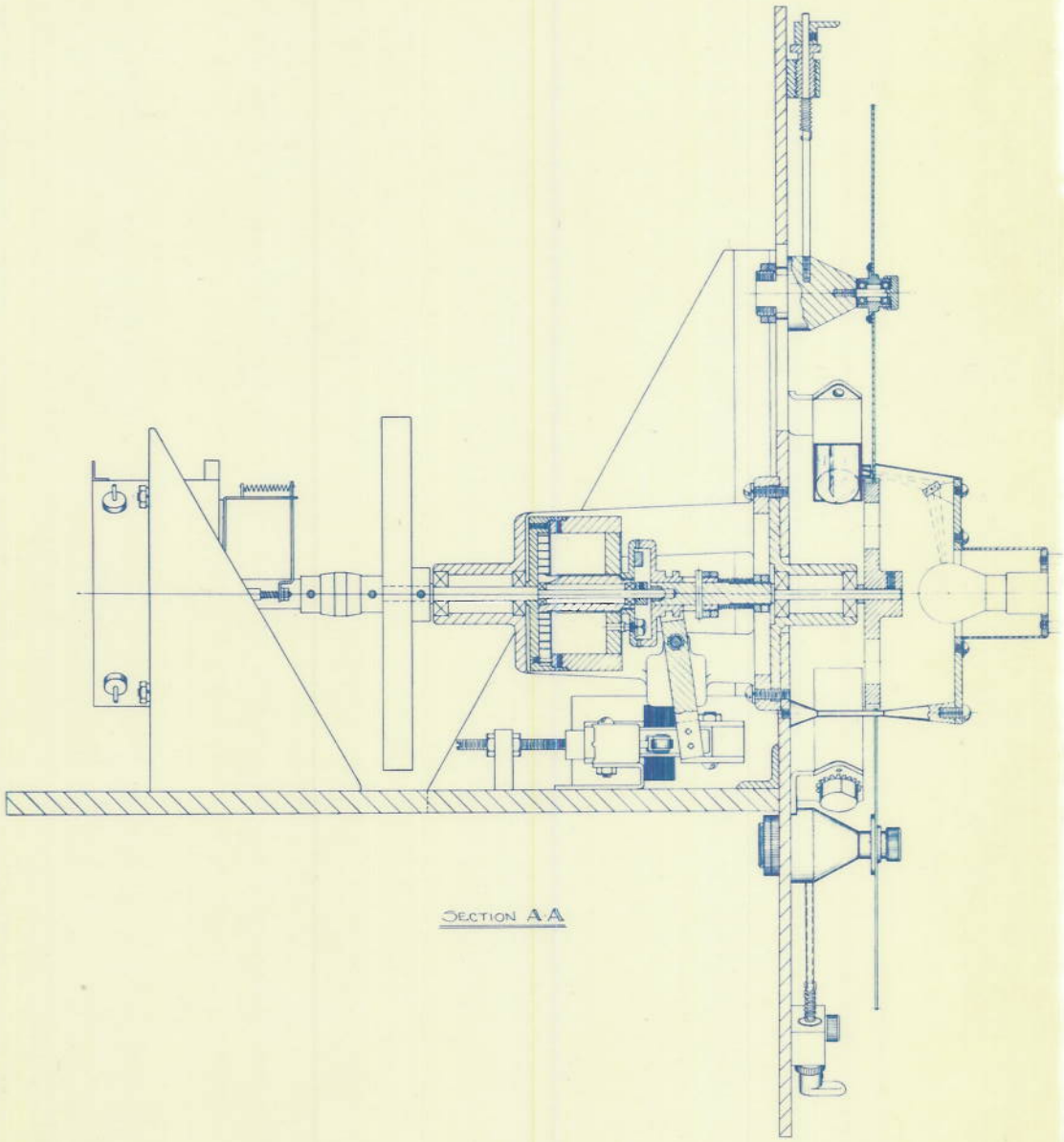
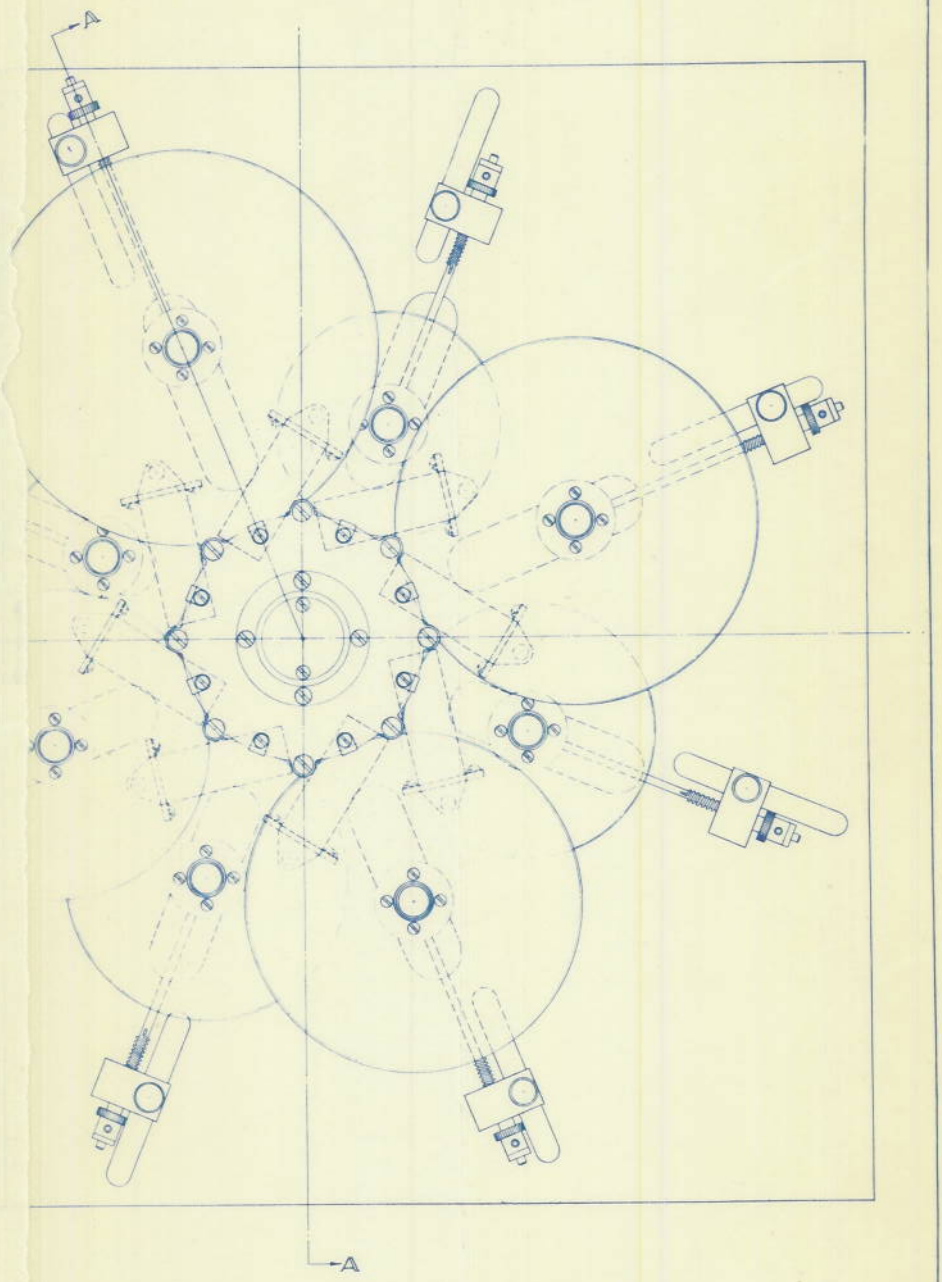
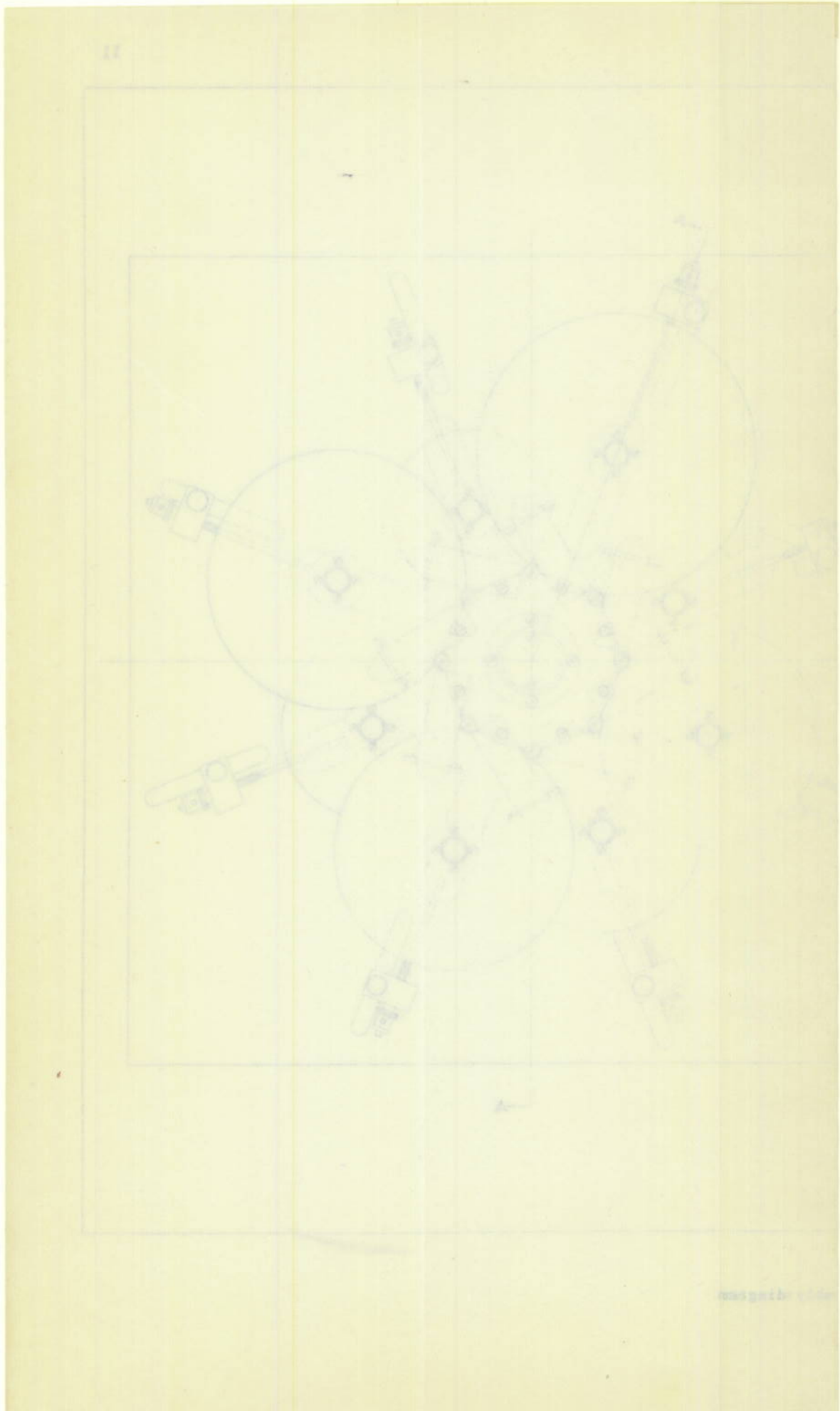


Figure 12. Proposed Code Ge


A
A



synchronous start equipment remain fundamentally the same as in the present model, although a more powerful drive motor would be desirable.

21. Figure 13 is the block diagram of the revised electronic circuits. The outputs from paired code disks are fed into electronic double-pole reversing switches, which, for a particular baud of cipher, feed the outputs from one of each pair of disks on to the cancellation circuits and the outputs from the other of each pair, except the last, to the succeeding switching circuit to control the switching action of that particular switch. A special cancellation circuit that receives its inputs from the last two disks of the group is used to control the first switch in the series. The other cancellation circuits are identical with those in the present model. In this way, sixteen separate cycles are simultaneously produced by the machine and the output is switched about among them more or less randomly from baud to baud. Also, the outputs from the disks that do the switching are not at the same instant present as a part of the code output. In the present experimental model, a code disk produces the same effect upon the output cycle independent of the position it occupies in the machine. However, in the proposed model, exchanging disks about from position to position would not change the cycle length but would completely change the nature of the cycle. With a set of 50 prime code disks there are approximately 500 million different cycle lengths available and in addition there are approximately 21 trillion separate and distinct cycles available from all possible combinations.

TESTS AND RESULTS

22. The synchronous start system for the experimental code generators has been tested under loop service conditions and it was found desirable to have the tripping delay in the receiving unit a little longer than in the transmitting unit, so that it is always possible to phase in only one direction to achieve exact synchronism. This is possible because the deviation between the tripping of the two clutches is not more than four milliseconds.

23. In loop test operation it was found that no more than five minutes is normally required to set up the code machine disks, start the machines, and achieve synchronism after the radio loop circuit had been properly established. The code machines will run indefinitely and automatically remain in proper phase if the communication link does not fail or become erratic.

24. The material shown in Figures 14 and 15 illustrates the ability of the experimental code generator to cover transmitted facsimile copy. Figure 15 is a stripped sample of a test chart in which one strip is encoded and decoded, the other two are pure cipher and enciphered copy. It is intriguing to endeavor to follow the printed matter into the adjacent strips and attempt to determine which one is pure cipher and which is covered printed matter. Figure 16 is also the strip type. The first strip is an encoded and decoded typewritten message; the second strip illustrates what happens when the code generators are operated one baud out of step.

25. Figures 17 to 23 are the results obtained with the NRL experimental code generator modified to give a weighted code so that the covering ability of other than 50-50 code could be evaluated. Figure 17 is the unencoded transmitted copy of an especially prepared test chart used in all the succeeding plates. Figure 18 has code weights of 39.1 per cent black to 60.9 per cent white on white copy and just the reverse on black copy. All of the parts of the test chart are discernible but the typewritten material is not legible. The pattern present is the result of the extensive modifications necessary in the code generating mechanism to produce a

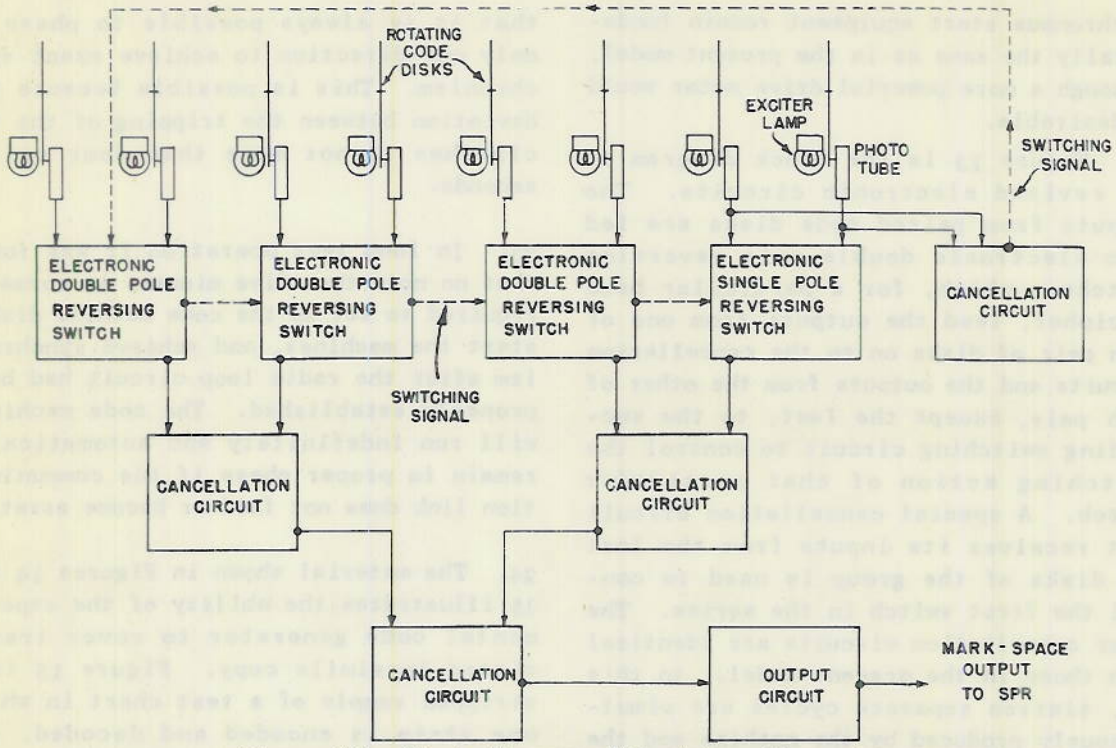


Figure 13. Block diagram of Prototype Generator

code that is this heavily weighted. Figure 19 has code weights of 46.8 per cent black to 53.2 per cent white. The large crosses still show quite clearly, the fine line figure has completely disappeared, and only a faint shadow remains of the typewritten material. Figure 20 has code weights of 47.7 to 52.3 per cent. Shadows of the broad crosses are still quite discernible but everything else has disappeared under the code. Figure 21 has code weights of 48.7 to 51.3 per cent. There is no obvious trace of any covered material in the positive print. However, when the negative was being processed, it was possible to see faint traces of the two broad crosses when the negative was held in the proper light, at an ideal angle, and observed at a distance of fifteen to twenty feet. Figure 22 has code weights of 49.1 to 50.9 per cent. At no time was it possible to detect visually the presence of any of the covered material in this plate. Figure 23 is a 50-50 code covering the test chart, and seems to be the only type safe enough for the transmission of highly classified copy.

CONCLUSIONS AND RECOMMENDATIONS

26. In view of the operating simplicity and efficiency, small physical size, and visual covering ability of the NRL experimental SPR code generator, it appears advantageous to extend the development and analysis of this type of device along the lines set forth in this report for an improved model. Considerable time would probably be required to achieve an accurate cryptographic evaluation of such a system; however, evaluation of designs should precede any further building of equipment.

ACKNOWLEDGMENT

27. Acknowledgment is made of the contributions of the Army Security Agency, the NRL Design and Drafting staff, Dr. O. Norgorden of the Communications Section of NRL, and Drs. C. E. Cleeton and J. E. Eaton of the Security Systems Section of NRL.

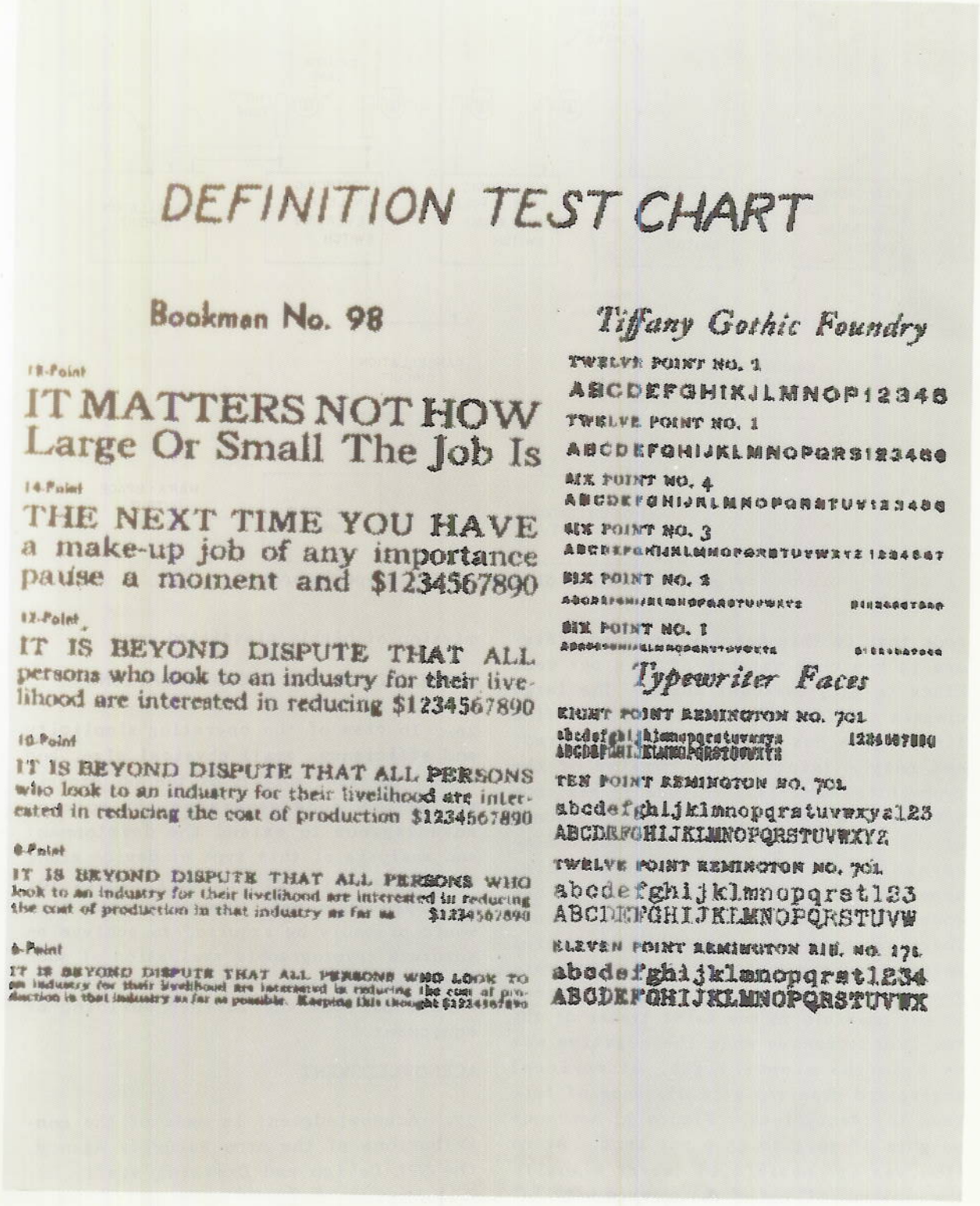


Figure 14. Transmitted Test Chart

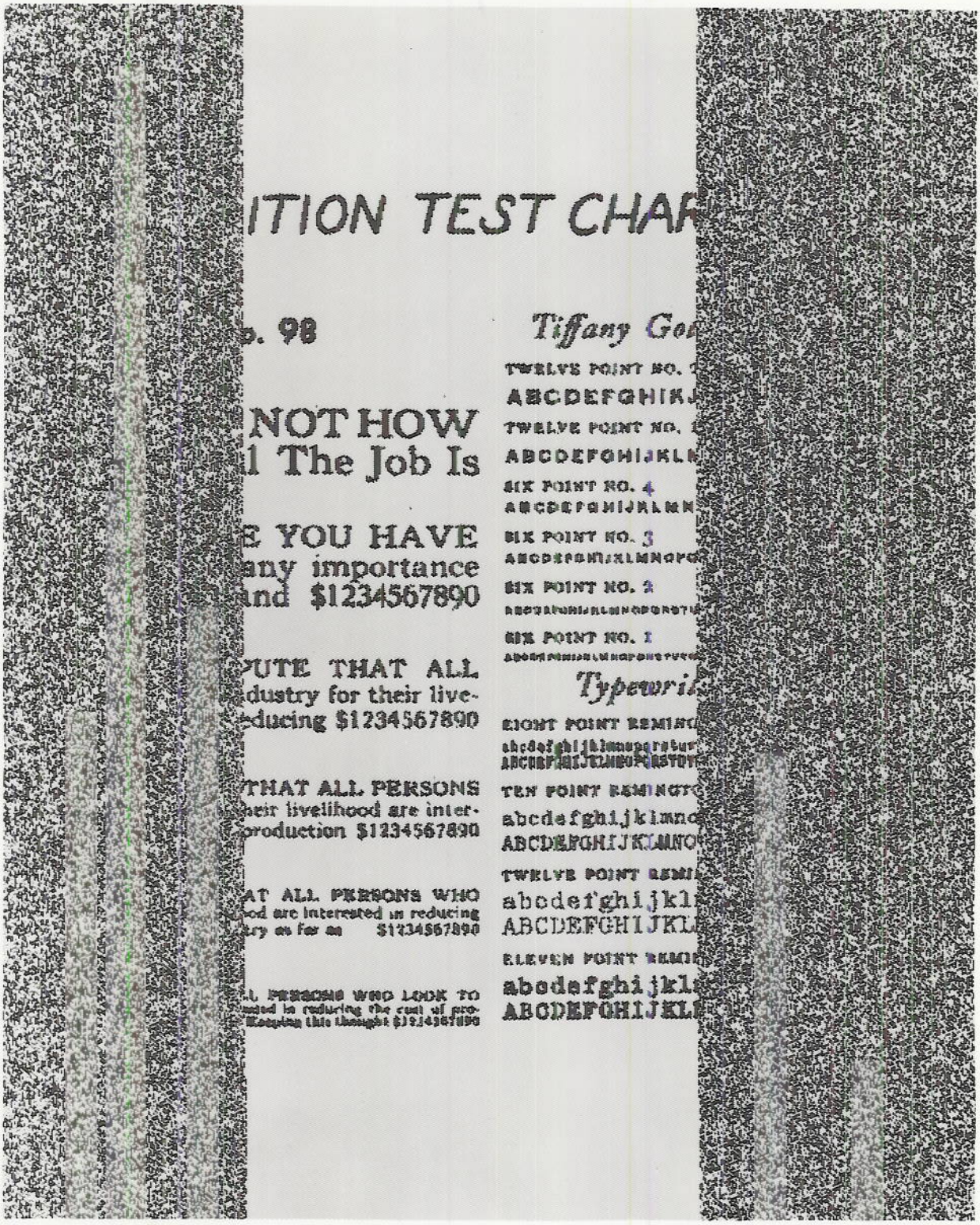


Figure 15. Stripped Test Chart

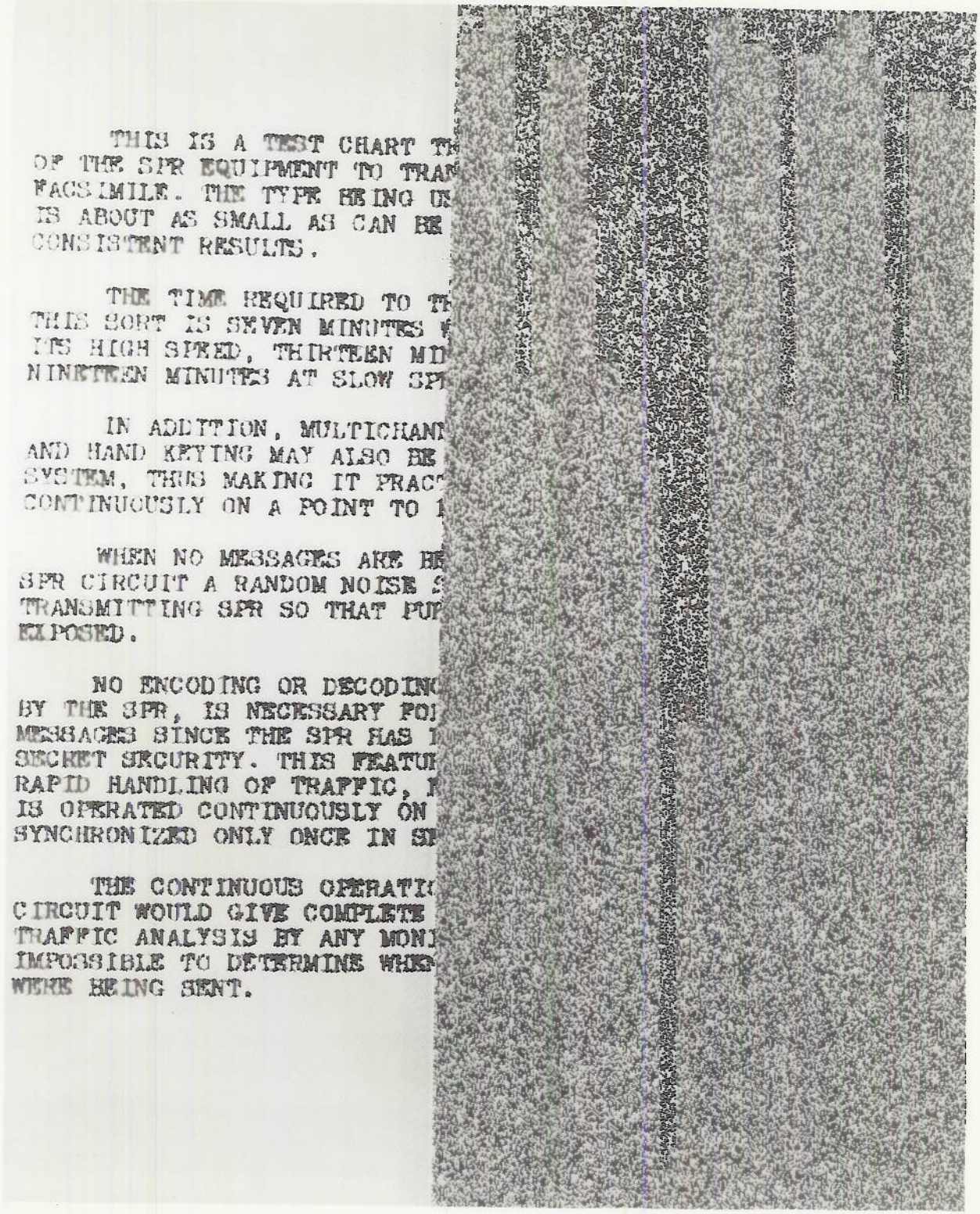


Figure 16. Stripped Test Chart

MEN MAY SAY WHAT THEY WILL IN PRAISE OF THEIR HOUSES AND GROW ELOQUENT UPON THE MERITS OF VARIOUS STYLES OF ARCHITECTURE, BUT FOR OUR PART WE ARE AGREED THAT THERE IS NOTHING SUPERIOR TO A TENT.

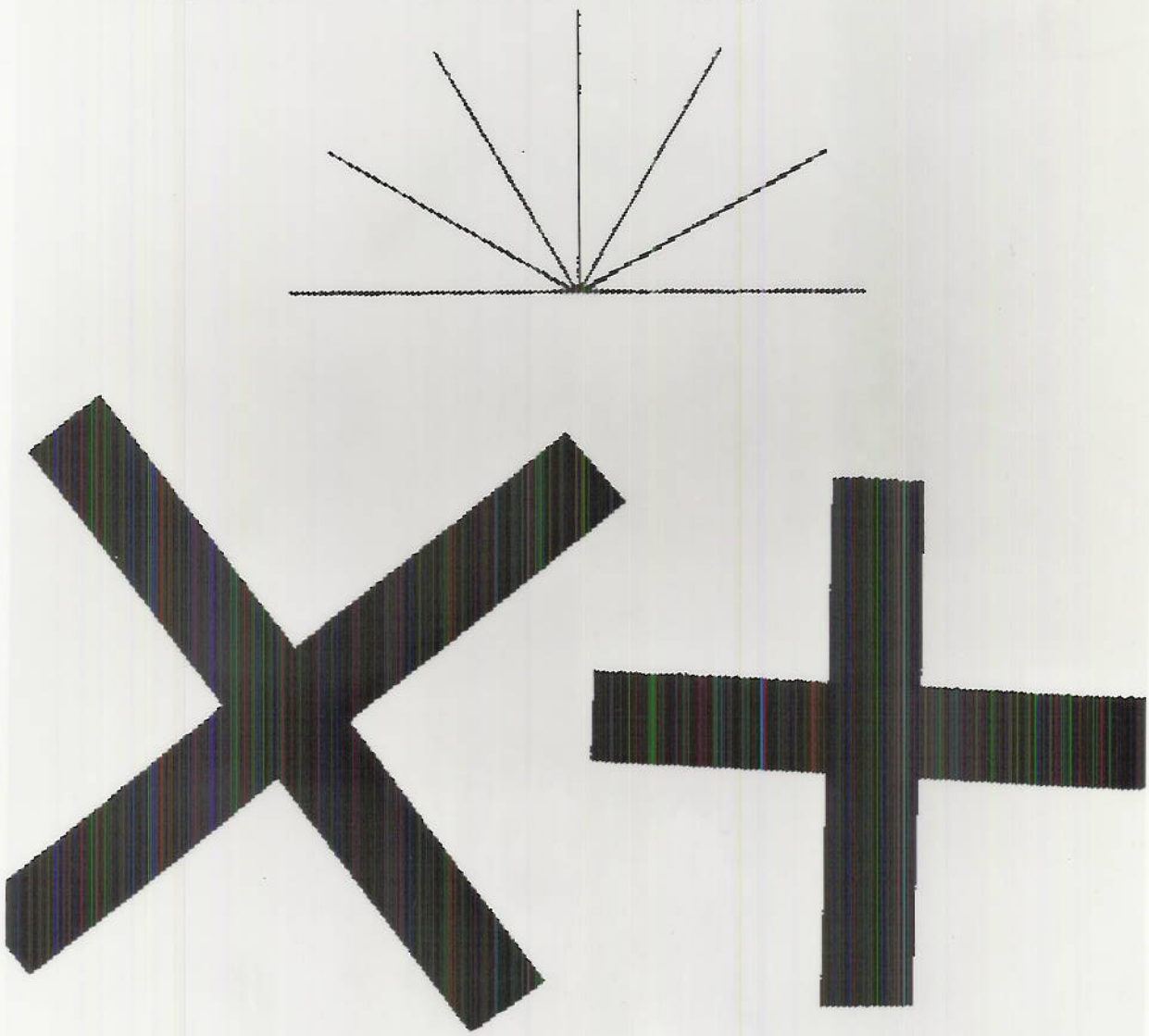


Figure 17. Special Test Chart

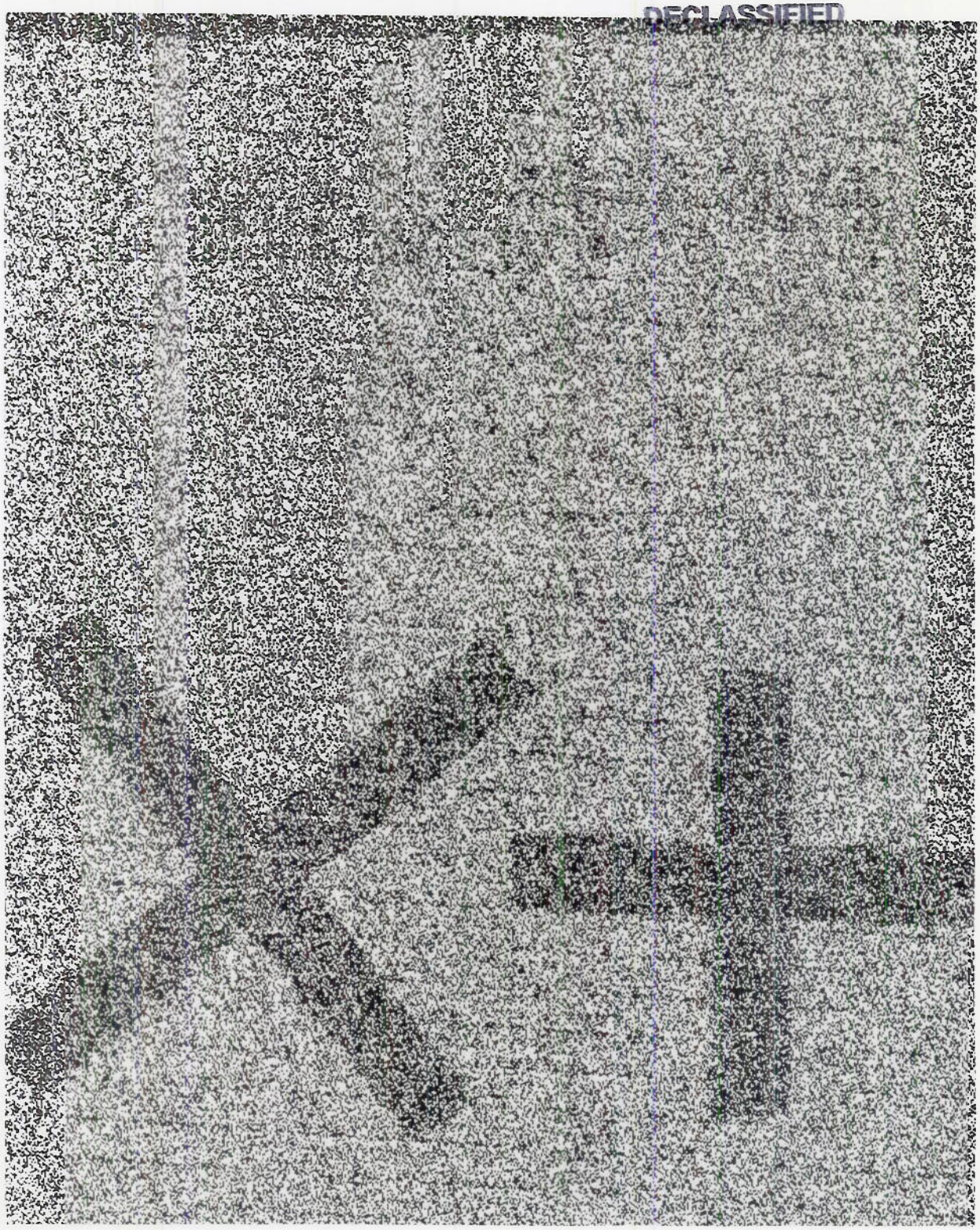


Figure 18. Weighted Sample No. 1

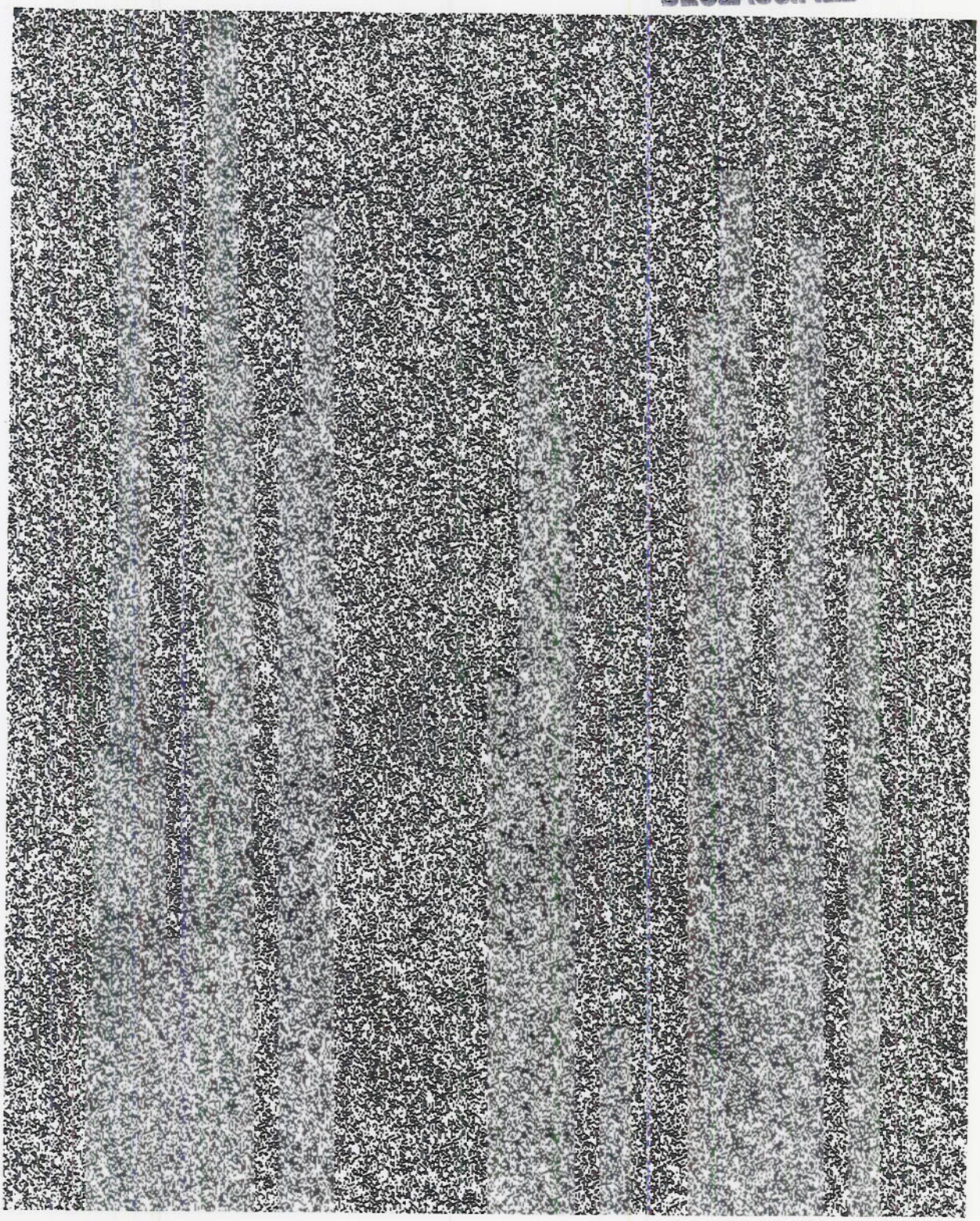


Figure 19. Weighted Sample No. 2

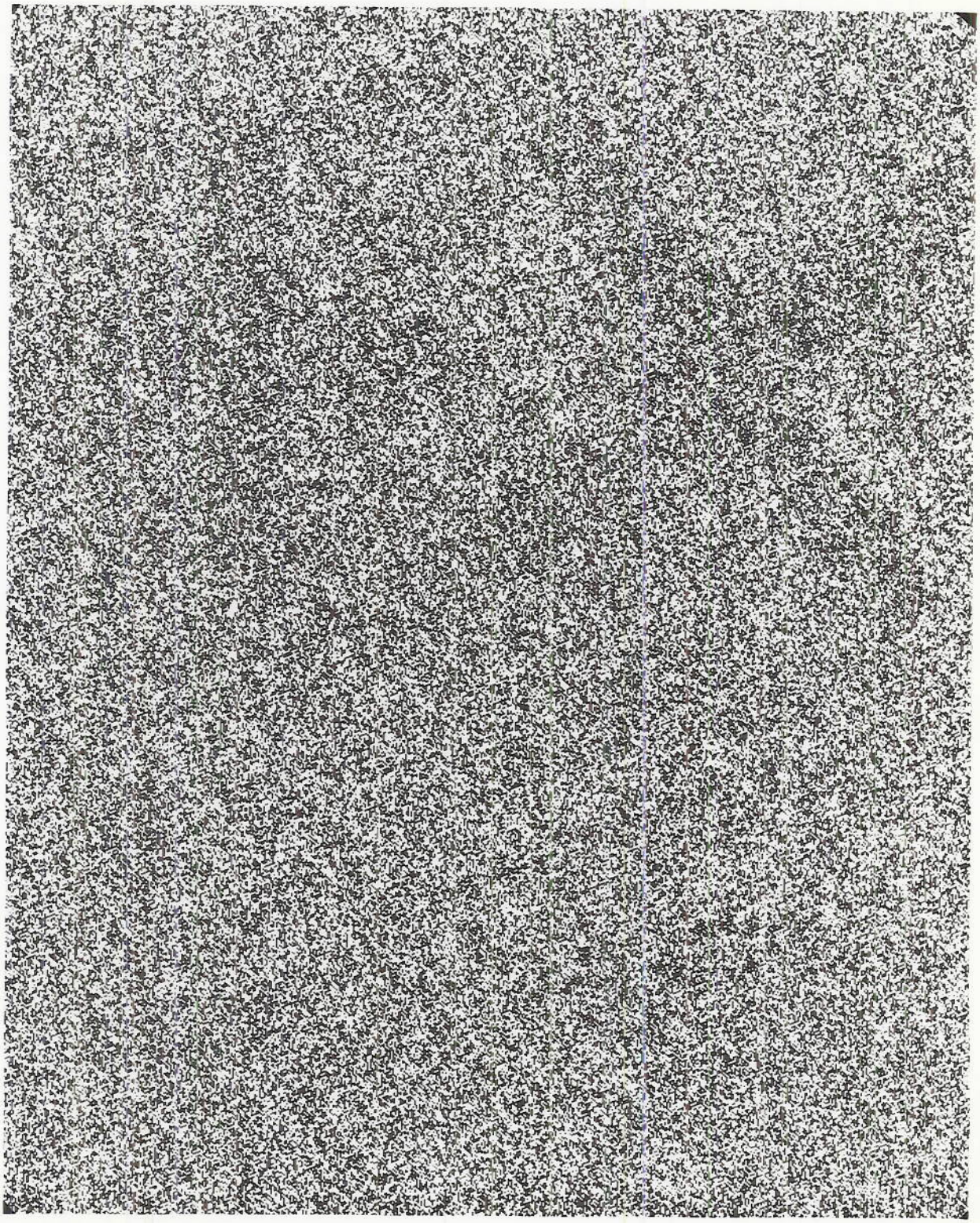


Figure 20. Weighted Sample No. 3

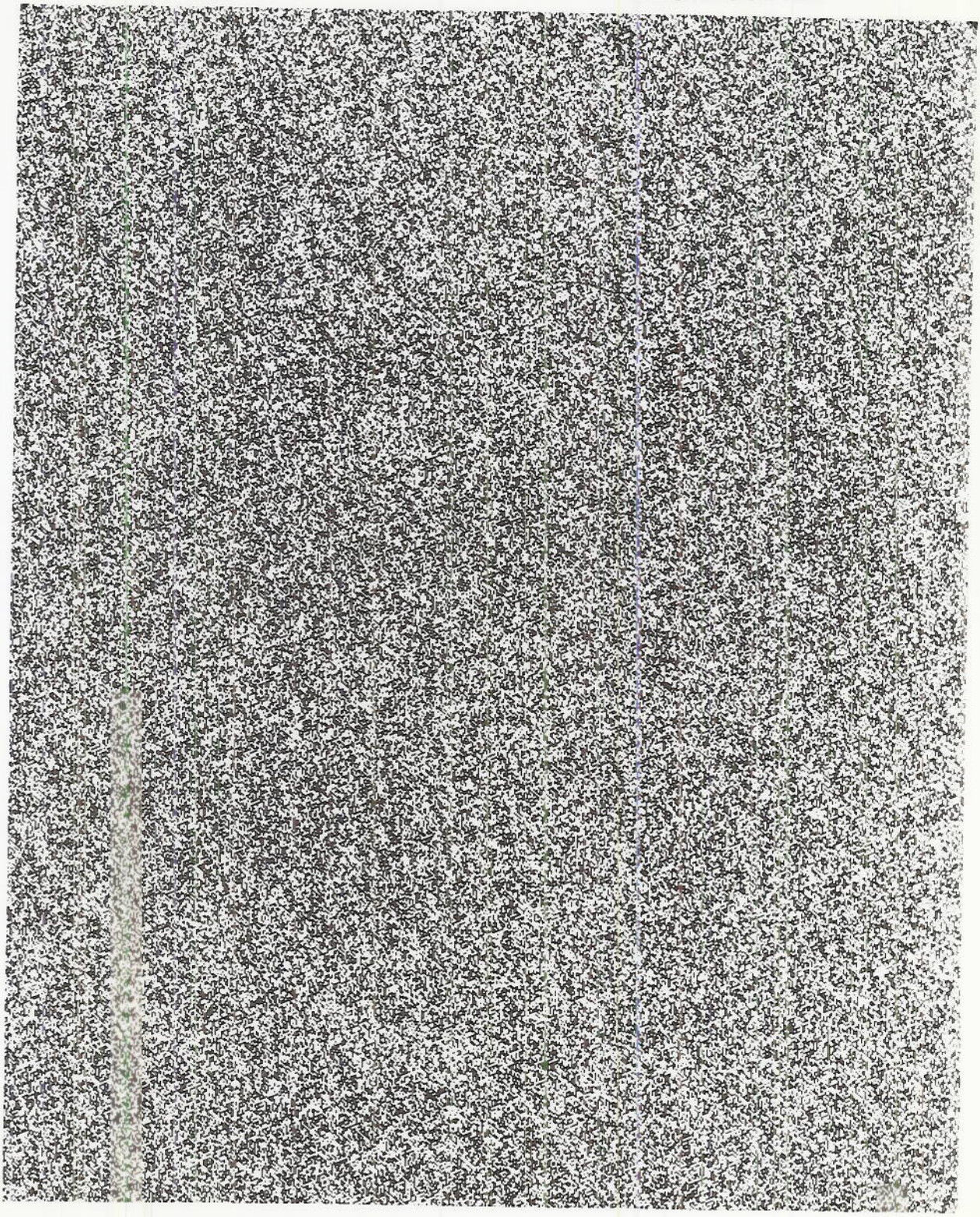


Figure 21. Weighted Sample No. 4

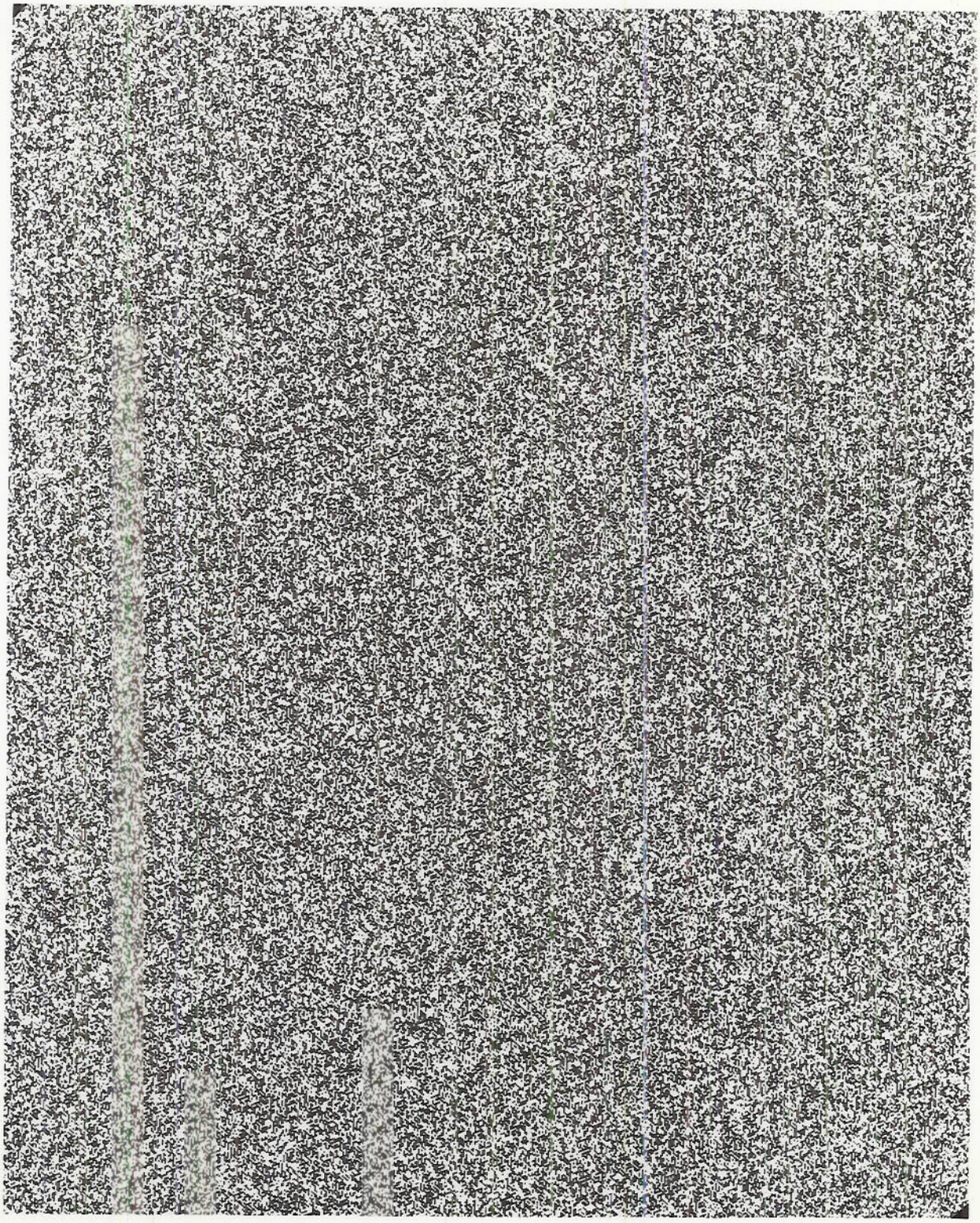


Figure 22. Weighted Sample No. 5

Figure 23. Half and Half Sample No. 6

APPENDIX I: Mathematical Evaluation of the NRL SPR Code Generators

1. The first point to be considered in the evaluation of a code generator to be used in a synchronous polarity-reversal system to cover facsimile copy is how nearly the average cipher output of the device approaches an ideal 50-50. In tests described in this report it was found that any cipher to be useful should not under any circumstances deviate as much as one per cent from a 50-50 average. In the test model of the NRL code generator, the outputs of five code disks are combined in four cancellation circuits that perform modulus-two addition of paired inputs, such that if no input is taken as "0" and an input is given the value of "1", then a cancellation circuit operates such that $0+0=0$, $1+0=1$, $0+1=1$, and $1+1=0$ will be the outputs. With the foregoing assumption for the operation of the cancellation circuits, the formula $a+b-2ab$ may be written to express the average code weight of the output from a single cancellation circuit if "a" is the decimal weight of one input and "b" is the decimal weight of the other input. Since the code disks used in a device of this type must be respectively prime, it becomes impossible to produce exactly a 50-50 code element distribution on them. Therefore, assume two of the disks used have code weights of 0.48 and 0.49, respectively, and are combined in a single cancellation circuit. Then the average output will be $0.48+0.49-2(0.48)(0.49)=0.97-0.4704=0.4996$. If this operation were repeated three more times with three more disks which have the same order of weight, the average of the total cycle would deviate by only a very small fraction of one percent from 50-50.

2. In the proposed generator, only three cancellation circuits are used to produce the output, so that even though the cipher output from the machine would not be quite as near to 50-50 as that of the experimental model, it would still be only a very small fraction of one percent from the desired 50-50 average.

3. The cycle length of the experimental model is equal to the product of the code elements on the five disks and equals 9,480,500,855 bauds of cipher, or enough cipher to last for a continuous period of 109.84 days if used at the rate of 1000 per second. However, this is not a good measure of the security of the device because it is possible to reestablish the code disk sequence from a continuous stretch of pure cipher which is one less than the sum of code elements of the five disks, or 494 continuous cipher units. This, of course, assumes that the number of code elements on each disk is known but not their distribution or relative settings. This method of attack is best shown by using an example employing three disks of lengths 5, 6, and 7 bauds. Since the sum of these three disks would be 18, a cipher length of only 17 continuous bauds is necessary to reestablish the code disks. The following equations of binary addition can be written if the first is designated "a", the second "b", and the third "c".

$$a_1+b_1+c_1=0 \quad (1)$$
$$a_2+b_2+c_2=0 \quad (2)$$
$$a_3+b_3+c_3=1 \quad (3)$$
$$a_4+b_4+c_4=0 \quad (4)$$
$$a_5+b_5+c_5=1 \quad (5)$$
$$a_1+b_6+c_6=1 \quad (6)$$
$$a_2+b_1+c_7=1 \quad (7)$$
$$a_3+b_2+c_1=0 \quad (8)$$

$$a_4+b_3+c_2=0 \quad (9)$$
$$a_5+b_4+c_3=0 \quad (10)$$
$$a_6+b_5+c_4=1 \quad (11)$$
$$a_2+b_6+c_5=0 \quad (12)$$
$$a_3+b_1+c_6=1 \quad (13)$$
$$a_4+b_2+c_7=1 \quad (14)$$
$$a_5+b_3+c_1=0 \quad (15)$$
$$a_1+b_4+c_2=1 \quad (16)$$
$$a_2+b_5+c_3=0 \quad (17)$$

In this system $0+0=0$, $1+1=0$, and therefore $a_1+a_1=0$ or $b_2+b_2=0$, and therefore if equation *(1)* and equation *(6)* are added, and equation *(2)* and equation *(7)* are added and so on, the following set of equations will be derived:

$$b_1+b_6+c_1+c_6=1 \quad (18)$$
$$b_2+b_1+c_2+c_7=1 \quad (19)$$
$$b_3+b_2+c_3+c_1=1 \quad (20)$$
$$b_4+b_3+c_4+c_2=0 \quad (21)$$
$$b_5+b_4+c_5+c_3=1 \quad (22)$$
$$b_6+b_5+c_6+c_4=0 \quad (23)$$
$$b_1+b_6+c_7+c_5=1 \quad (24)$$
$$b_2+b_1+c_1+c_6=1 \quad (25)$$
$$b_3+b_2+c_2+c_7=1 \quad (26)$$
$$b_4+b_3+c_3+c_1=0 \quad (27)$$
$$b_5+b_4+c_4+c_2=0 \quad (28)$$
$$b_6+b_5+c_5+c_3=0 \quad (29)$$

If equations *(18)* through *(23)* are added the "*b*" terms all drop out so that the equation derived is:

$$c_5+c_7=0 \quad (30)$$

This means that c_5 and c_7 are the same and both are either 0 or 1. To continue the addition of the above equations six at a time the following set of equations is secured:

$$c_5+c_7=0 \quad (30)$$
$$c_6+c_1=0 \quad (31)$$

$$c_7+c_2=0 \quad (32)$$
$$c_1+c_3=0 \quad (33)$$
$$c_2+c_4=0 \quad (34)$$
$$c_3+c_5=1 \quad (35)$$
$$c_4+c_6=1 \quad (36)$$

By combining equations *(30)* to *(36)* it is found that:

$$c_1=(1+c_2)=c_3=(1+c_4)=(1+c_5)=c_6=(1+c_7) \quad (37)$$

When these values are substituted into equations *(18)* to *(23)* the following equations are produced:

$$b_1+b_6=1 \quad (38)$$
$$b_2+b_1=1 \quad (39)$$
$$b_3+b_2=1 \quad (40)$$
$$b_4+b_3=0 \quad (41)$$
$$b_5+b_4=0 \quad (42)$$
$$b_6+b_5=1 \quad (43)$$

By combining equations *(38)* to *(43)*, it is found that:

$$b_1=(1+b_2)=b_3=b_4=b_5=(1+b_6) \quad (44)$$

When the values of *(37)* and *(44)* are substituted in equations *(1)* to *(5)*, the following values of "*a*" are obtained:

$$a_1=a_2(1+a_3)=(1+a_4)=a_5 \quad (45)$$

Given equations *(37)*, *(44)*, and *(45)*, it is now possible to write all the values of "*a*", "*b*", and "*c*".

4. It would seem at first thought that if a set of fifty prime disks were used to fill the five positions in the machine that the problem of finding the proper combination out of the 2,118,760 possible combinations available would be prohibitive because of the considerable time that would be needed to check each possible solution, even with the aid of the best available calculating machines. However, since the mathematical process

that is employed in the device is purely additive, it would be possible to write equations of the type illustrated above which would include all possible prime disks that could be used in a given machine. Thus, if a machine were equipped with a set of fifty prime code disks, it would be possible to write equations containing fifty unknowns each. Using equations of this sort, a total of equations equal to the total number of code elements of the entire set of disks would be required, or approximately 7500 continuous bauds of pure cipher. The solution to this problem would give the particular disks in use, their code element arrangement, and the starting point of each. All disks not in use would come out to be zero at all points. To make a solution of this type, it would be necessary to use a digital type of electronic calculating machine. After the original set of equations had been established, a solution with the aid of the calculating machine would be a relatively short process.

5. If in the improved model code generator described in paragraphs 20 and 21 of the report, the code disks are designated respectively "*a*", "*b*", "*c*", "*d*", "*e*", "*f*", "*g*", and "*h*", then the following equation in modulus-two addition may be written to represent the output of the machine (k):

$$b_1+d_1+f_1+h_1+a_1g_1+a_1h_1+a_1c_1+a_1d_1+b_1g_1+b_1h_1+c_1e_1+c_1f_1+e_1g_1+e_1h_1+a_1c_1g_1+a_1c_1h_1+a_1d_1g_1+a_1d_1h_1+a_1c_1e_1+a_1d_1e_1+a_1c_1f_1+a_1d_1f_1+b_1c_1g_1+b_1c_1h_1+b_1d_1g_1+b_1d_1h_1+c_1e_1g_1+c_1f_1g_1+c_1e_1h_1+c_1f_1h_1+a_1c_1e_1g_1+a_1c_1e_1h_1+a_1d_1e_1h_1+a_1c_1f_1g_1+a_1d_1f_1g_1+a_1d_1e_1g_1+a_1c_1f_1h_1+a_1d_1f_1h_1=k_1 \qquad (46)$$

In this equation the subscripts indicate a particular code element on each of the lettered code disks. The product terms of this equation rule out the possibility of establishing equations that include all possible code disks that could be used in the machine, and therefore a direct attack on the whole system at one time with digital calculating machines would be impossible. The most logical approach left is a probability attack in which the proper set of eight disks would be arrived at by trial and error. The problem is further complicated by the fact that the eight disks used must be in the proper positions in the machine to give a particular cipher output, so that the selection of the correct eight would be involved with their correct positioning.

6. The amount of pure cipher necessary to make any attack possible is best arrived at by again using a simplified example as follows: Let us assume code disks "*a*" and "*b*" with the output switched from one to the other by the output from a third code disk "*x*". This type of device produces product terms in its equations which have characteristics as follows: $0\times0=0$, $1\times0=0$, $1\times1=1$, and $a_1\times a_1=a_1$. With this arrangement in mind the following set of equations could be written to represent the output from such a device:

$$a_1x_1+b_1+b_1x_1=0 \qquad (47)$$
$$a_2x_2+b_2+b_2x_2=1 \qquad (48)$$
$$a_3x_3+b_3+b_3x_3=1 \qquad (49)$$
$$a_4x_4+b_4+b_4x_4=0 \qquad (50)$$
$$a_5x_5+b_5+b_5x_5=1 \qquad (51)$$
$$a_1x_6+b_6+b_6x_6=0 \qquad (52)$$
$$a_2x_7+b_1+b_1x_7=0 \qquad (53)$$
$$a_3x_1+b_2+b_2x_1=1 \qquad (54)$$
$$a_4x_2+b_3+b_3x_2=0 \qquad (55)$$
$$a_5x_3+b_4+b_4x_3=0 \qquad (56)$$
$$a_1x_4+b_5+b_5x_4=1 \qquad (57)$$
$$a_2x_5+b_6+b_6x_5=1 \qquad (58)$$
$$a_3x_6+b_1+b_1x_6=1 \qquad (59)$$
$$a_4x_7+b_2+b_2x_7=1 \qquad (60)$$
$$a_5x_1+b_3+b_3x_1=0 \qquad (61)$$
$$a_1x_2+b_4+b_4x_2=0 \qquad (62)$$
$$a_2x_3+b_5+b_5x_3=0 \qquad (63)$$

$$a_3x_4+b_6+b_6x_4=1 \quad (64)$$
$$a_4x_5+b_1+b_1x_5=0 \quad (65)$$
$$a_5x_6+b_2+b_2x_6=0 \quad (66)$$
$$a_1x_7+b_3+b_3x_7=0 \quad (67)$$
$$a_2x_1+b_4+b_4x_1=0 \quad (68)$$
$$a_3x_2+b_5+b_5x_2=1 \quad (69)$$
$$a_4x_3+b_6+b_6x_3=1 \quad (70)$$
$$a_5x_4+b_1+b_1x_4=0 \quad (71)$$
$$a_1x_5+b_2+b_2x_5=1 \quad (72)$$
$$a_2x_6+b_3+b_3x_6=0 \quad (73)$$
$$a_3x_7+b_4+b_4x_7=0 \quad (74)$$
$$a_4x_1+b_5+b_5x_1=1 \quad (75)$$
$$a_5x_2+b_6+b_6x_2=1 \quad (76)$$
$$a_1x_3+b_1+b_1x_3=0 \quad (77)$$
$$a_2x_4+b_2+b_2x_4=1 \quad (78)$$
$$a_3x_5+b_3+b_3x_5=1 \quad (79)$$
$$a_4x_6+b_4+b_4x_6=1 \quad (80)$$
$$a_5x_7+b_5+b_5x_7=1 \quad (81)$$
$$a_1x_1+b_6+b_6x_1=0 \quad (82)$$
$$a_2x_2+b_1+b_1x_2=0 \quad (83)$$
$$a_3x_3+b_2+b_2x_3=1 \quad (84)$$
$$a_4x_4+b_3+b_3x_4=0 \quad (85)$$
$$a_5x_5+b_4+b_4x_5=0 \quad (86)$$
$$a_1x_6+b_5+b_5x_6=0 \quad (87)$$
$$a_2x_7+b_6+b_6x_7=1 \quad (88)$$
$$a_3x_1+b_1+b_1x_1=1 \quad (89)$$
$$a_4x_2+b_2+b_2x_2=1 \quad (90)$$
$$a_5x_3+b_3+b_3x_3=0 \quad (91)$$
$$a_1x_4+b_4+b_4x_4=0 \quad (92)$$
$$a_2x_5+b_5+b_5x_5=1 \quad (93)$$
$$a_3x_6+b_6+b_6x_6=1 \quad (94)$$
$$a_4x_7+b_1+b_1x_7=0 \quad (95)$$

It will be noted that no definite information can be derived directly from this set of equations until after equation 77 has been reached, at which point "a" and "b" have completed a cycle with respect to each other. Even here information with respect to "a" and "b" will be in terms of whether "a" and "b" terms are respectively opposite to each other when the sum of equations like (50) and (80) are equal to one. It will be found that a very long sampling of this type would be necessary to solve for all values of "a", "b", and "x". If equations (47) and (82) are added, and so on with successive equations where "a" and "x" have completed one cycle, then the sums that are equal to one will give definite values for "x" and relative values for "b" as follows (beginning with equation (47) plus equation (82)):

$$b_1+b_6+b_1x_1+b_6x_1=(x_1+1)(b_6+b_1)=0 \quad (96)$$
$$b_2+b_1+b_2x_2+b_1x_2=(x_2+1)(b_1+b_2)=1 \quad (97)$$
$$b_3+b_2+b_3x_3+b_2x_3=(x_3+1)(b_2+b_3)=0 \quad (98)$$
$$b_4+b_3+b_4x_4+b_3x_4=(x_4+1)(b_3+b_4)=0 \quad (99)$$
$$b_5+b_4+b_5x_5+b_4x_5=(x_5+1)(b_4+b_5)=1 \quad (100)$$
$$b_6+b_5+b_6x_6+b_5x_6=(x_6+1)(b_5+b_6)=0 \quad (101)$$
$$b_1+b_6+b_1x_7+b_6x_7=(x_7+1)(b_6+b_1)=1 \quad (102)$$
$$b_2+b_1+b_2x_1+b_1x_1=(x_1+1)(b_1+b_2)=0 \quad (103)$$
$$b_3+b_2+b_3x_2+b_2x_2=(x_2+1)(b_2+b_3)=1 \quad (104)$$
$$b_4+b_3+b_4x_3+b_3x_3=(x_3+1)(b_3+b_4)=0 \quad (105)$$
$$b_5+b_4+b_5x_4+b_4x_4=(x_4+1)(b_4+b_5)=1 \quad (106)$$

In equation (97), $x_2+1=1$ and $b_1+b_2=1$, therefore $x_2=0$ and b_1 and b_2 are opposite. Likewise from equation (100), $x_5=0$ and $b_4=b_5+1$; in equation (102) $x=0$ and $b_1=b_6+1$; in equation (104) $x_2=0$ and $b_2=b_3+1$; and in equation (106) $x_4=0$ and $b_4=b_5+1$. Going into equation (96), it has been found that $b_1+b_6=1$ and therefore $x_1+1=0$ and therefore $x_1=1$. Likewise in equation (98) it can be shown that $x_3=1$. Now then, if equations (47) and (89) are added, and so on (that is, the equations in which one cycle between "x" and "b" has been completed) then the following set of equations is produced:

$$x_1(a_1+a_3)=1 \quad (107)$$
$$x_2(a_2+a_4)=0 \quad (108)$$
$$x_3(a_3+a_5)=1 \quad (109)$$
$$x_4(a_4+a_1)=0 \quad (110)$$
$$x_5(a_5+a_2)=0 \quad (111)$$

$$x_6(a_1+a_3)=1 \qquad (112)$$

$$x_7(a_2+a_4)=0 \qquad (113)$$

From equation *(107)* it can be seen that $x_1=1$; from equation *(109)* that $x_3=1$; and from equation *(112)* that $x_6=1$. Therefore the values of "x" are: $x_1=1$, $x_2=0$, $x_3=1$, $x_4=0$, $x_5=0$, $x_6=1$, and $x_7=0$. Beginning with equation *(47)* and substituting in values that have been found for "x", it is found that $a_1=0$, in equation *(48)* $b_2=1$, in equation *(49)* $a_3=1$, in equation *(50)* $b_4=0$, in equation *(51)* $b_5=1$, in equation *(53)* $b_1=0$, in equation *(55)* $b_3=0$, in equation *(56)* $a_5=0$, in equation *(58)* $b_6=1$, in equation *(63)* $a_2=0$, and from equation *(70)* $a_4=1$. This represents one method of solution for this problem, but there are other procedures that would work equally well; however, approximately the same number of equations would be required. This solution indicates that it is necessary to have a length of cipher which is longer than the product of the letters of the longest terms.

7. There are eight terms that are made up of four letters, sixteen terms that are made up of three letters, ten terms with two letters each, and four terms with one letter each. If the equation is analyzed, it will be found that the sum of the terms containing four letters will add up to be zero an average of 25/32 of the time, and therefore it might be possible to drop these terms and work only with the terms containing three letters or less. It would then be only necessary to use a length of pure code signal that would be sufficiently longer than the product of any three disks to be able to eliminate the errors introduced by the dropped terms. This would probably require a length of more than 10^7 bauds or somewhat in excess of 100 minutes. This This type of solution assumes, of course, that the code disks in use and their exact positions are known, but not the code arrangement of the individual disks or their initial settings.

8. If, in the code generator described in paragraphs 20 and 21 of the report, the last two code disks are used to control only the first switch circuit, and do not contribute to the output circuits, the equation for the output of the device would become:

$$b_1+d_1+f_1+a_1g_1+a_1h_1+a_1c_1+a_1d_1+b_1g_1+b_1h_1+c_1e_1+c_1f_1+a_1c_1g_1+a_1c_1h_1+a_1d_1g_1+a_1d_1h_1+a_1c_1e_1+a_1d_1e_1+a_1c_1f_1+a_1d_1f_1+b_1c_1g_1+b_1c_1h_1+b_1d_1g_1+b_1d_1h_1+a_1c_1e_1g_1+a_1c_1e_1h_1+a_1d_1e_1g_1+a_1d_1e_1h_1+a_1c_1f_1g_1+a_1c_1f_1h_1+a_1d_1f_1g_1+a_1d_1f_1h_1+b_1c_1e_1g_1+b_1c_1e_1h_1+b_1d_1e_1g_1+b_1d_1e_1h_1+b_1c_1f_1g_1+b_1c_1f_1h_1+b_1d_1f_1g_1+b_1d_1f_1h_1=k \qquad (114)$$

There are sixteen terms of four letters each in this equation. The average output from these sixteen terms will average to be zero 43/64 of the time, which would make it practically impossible to ignore these terms in the solution of the equation. Therefore the length of cipher necessary to break this code would be at least 10^8 bauds, or in excess of twenty-four hours of pure cipher. However, only two cancellation circuits would be used in this circuit arrangement and therefore the average cipher output might not average near enough to 50-50 to be entirely safe against visual attack. Also, this arrangement is more susceptible to a statistical attack and therefore it is probably no better than, if as good as, the first system.

9. In evaluating the security of the proposed code generator, it must be kept in mind that the calculations presented in the preceding paragraphs have been worked out on the assumption that the number of elements in each code disk in use is known. However, with a set of 50 prime disks available, there are 21 trillion combinations available with 500 million different cycle lengths. The aforementioned calculations give no aid in determining the particular code disks

in use or their respective positions, and as far as has been found this could be determined only by trial and error procedure, which, considering the number of available combinations, would seem to rule out a direct mathematical attack upon the system.