WORD ERROR RATES IN CRYPTOGRAPHIC ENSEMBLES

D. J. Torrieri

Naval Research Laboratory
Washington, D. C.

4 October 1973

Security Classification

AD 769458

DOCUMENT CONTROL DATA - R & D

(Security classification of title, body of abstract and indexing annotation must be entered when the overall report is classified)

1. ORIGINATING ACTIVITY *(Corporate author)*
Naval Research Laboratory
Washington, D.C. 20375

2a. REPORT SECURITY CLASSIFICATION
Unclassified

2b. GROUP

3. REPORT TITLE
WORD ERROR RATES IN CRYPTOGRAPHIC ENSEMBLES

4. DESCRIPTIVE NOTES *(Type of report and inclusive dates)*
A final report on one phase of the NRL Problem.

5. AUTHOR(S) *(First name, middle initial, last name)*
D.J. Torrieri

6. REPORT DATE
October 4, 1973

7a. TOTAL NO. OF PAGES
15

7b. NO. OF REFS
5

8a. CONTRACT OR GRANT NO.
NRL Problem R06-55

b. PROJECT NO.
ND02.01.D

c.

d.

9a. ORIGINATOR'S REPORT NUMBER(S)
NRL Report 7616

9b. OTHER REPORT NO(S) *(Any other numbers that may be assigned this report)*

10. DISTRIBUTION STATEMENT
Approved for public release; distribution unlimited.

11. SUPPLEMENTARY NOTES

12. SPONSORING MILITARY ACTIVITY
Department of the Navy
Naval Air Systems Command
Washington, D.C. 20360

13. ABSTRACT

The word error rate of an ensemble of cryptographic systems is determined The word error rate is specified as a function of the corresponding plain-text bit error rate. Degradation is defined and computed for the case of phase shift keying and white Gaussian noise. Finally, the effect of differential encoding on a cryptographic system is investigated.

DD FORM 1 NOV 68 1473 (PAGE 1)

S/N 0101-807-6801

Security Classification

Security Classification

14 KEY WORDS	LINK A		LINK B		LINK C	
	ROLE	WT	ROLE	WT	ROLE	WT
Cryptography						
Enciphering						
Deciphering						
Word error rate						
Bit error rate						

DD FORM 1 NOV 68 1473 (BACK)
(PAGE 2)

Security Classification

U. S. GOVERNMENT PRINTING OFFICE : 1973—542-166/Z-114

CONTENTS

ABSTRACT

The word error rate of an ensemble of cryptographic systems is determined. The word error rate is specified as a function of the corresponding plain-text bit error rate. Degradation is defined and computed for the case of phase shift keying and white Gaussian noise. Finally, the effect of differential encoding on a cryptographic system is investigated.

Manuscript submitted May 23, 1973.

WORD ERROR RATES IN CRYPTOGRAPHIC ENSEMBLES

INTRODUCTION

In any digital communication system, the transmitted bits and words have certain error rates. When the digital bits are enciphered but the other system parameters remain unchanged, these error rates increase. It is the object of this report to obtain theoretically a quantitative measure of this degradation.

A standard enciphering technique is the modulo-2 addition of the plain text with a pseudorandom code sequence. Figure 1 shows an implementation in which a four-stage feedback shift register and exclusive OR gates are used. For each distinct setting of the switches, there is a different enciphered output stream. The corresponding deciphering system is shown in Fig. 2, where the switches must be set in the same manner as those of the enciphering system. A detailed discussion of this type of cryptographic method can be found in the literature (1-4).

Qualitatively, the reason for the degradation in cryptographic systems is due to the presence of shift registers in the enciphering and deciphering mechanisms. A bit error due to random noise will be carried through a shift register, causing additional bit errors down the line.

GENERAL DISCUSSION

The bit error rate for ordinary transmission is a function of the modulation system. For most modulation systems, when white Gaussian noise is present, the bit error rate has the functional form specified by

$$P_b = f\left(\frac{E_b}{N_0}\right) \tag{1}$$

where f is a function, N_0 is the noise power spectral density, and E_b is the mean energy for a bit in the ONE state. Assuming that bit errors occur independently of each other, the associated word error rate is

$$P_w = 1 - (1 - P_b)^k, \tag{2}$$

where k denotes the number of bits per word.

It is shown in the next section that the corresponding formulas for cryptographic bits and words are

$$\overline{P}_{cb} = P_b\,(1 - P_b)^{n-1} + 1/2\,(1 + P_b)\left[1 - (1 - P_b)^{n-1}\right]; \tag{3}$$

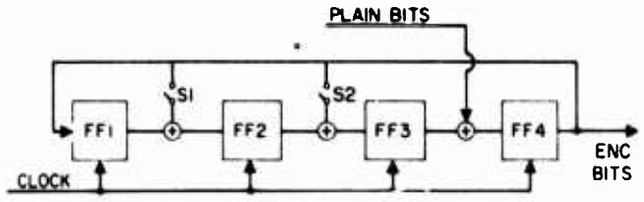

Fig. 1 — Typical enciphering system

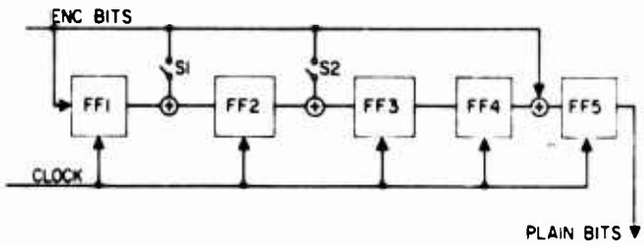

Fig. 2 — Corresponding deciphering system

$$\overline{P}_{cw} = \left[1 - 2^{-k}\,(1 - P_b)^k\right]\,\left[1 - (1 - P_b)^{n-k}\right] + \sum_{i=1}^{k-1} P_b \left[1 - 2^{-i}(1 - P_b)^k\right]\,(1 - P_b)^{n-i-1} + \left[1 - (1 - P_b)^k\right]\,(1 - P_b)^{n-1}, \qquad n > k; \tag{4a}$$

$$\overline{P}_{cw} = \sum_{i=1}^{n-1} P_b \left[1 - 2^{-i}(1 - P_b)^k\right]\,(1 - P_b)^{n-i-1} + \left[1 - (1 - P_b)^k\right]\,(1 - P_b)^{n-1}, \qquad n \leq k, \tag{4b}$$

where $\overline{P}_{cb}$ and $\overline{P}_{cw}$ are the ensemble average error rates of a cryptographic bit and a cryptographic word respectively. In these formulas, n denotes the number of bits affected by an initial bit error. For example, in the linear system of Figs. 1 and 2 an initial bit error at the input of the deciphering system is carried by the shift register until $n - 1$ more bits are received. Thus n is equal to the number of shift-register stages in the usual linear system.

It is immediately noticed that the cryptographic-error-rate formulas are written as functions of the bit error rate due to random noise. If Eq. (1) is substituted into Eqs. (3) and (4), there result formulas in terms of E_b. By comparing these formulas with Eqs. (1) and (2), we can determine the increase in E_b required for enciphered bits or words to maintain the same error rates as plain bits or words. This increase provides a quantitative measure of cryptographic degradation.

The cryptographic-error-rate formulas are very tedious to use in manual computations. In many cases, approximate formulas are highly accurate over the range of interest. It is shown in the next section that the following approximations can be used:

$$P_w \approx kP_b; \tag{5}$$

$$\overline{P}_{cb} \approx \left(\frac{n+1}{2}\right) P_b; \tag{6}$$

$$\overline{P}_{cw} \approx \begin{cases} [n + k - 2 - 2^{-k}(n - k - 2)]\ P_b, & n > k; \\ [n + k - 2 + 2^{-(n-1)}]\ P_b, & n \leq k. \end{cases} \tag{7}$$

A sufficient condition under which these equations are accurate for $n > 1$ is

$$P_b \ll \min\{n^{-1}, k^{-1}\}, \tag{8}$$

where the notation indicates that P_b must be much less than the smaller of the two quantities in the braces.

PROOF OF THE CRYPTOGRAPHIC ERROR RATE FORMULAS

Suppose an enciphered bit is erroneously received as a result of random noise or other interference. As the erroneous bit proceeds through the deciphering system, each of the next $n - 1$ bits will be affected. We define a "train" as a set of n consecutive enciphered bits, the first of which has been erroneously received due to interference.

The probability of error for each bit of a train could be computed for any specific deciphering system, e.g., the system of Fig. 2 with the switch settings specified. However, this computation would have to be repeated each time the configuration of the deciphering system is altered. Therefore, a more useful approach is to consider the ensemble of all possible cryptographic systems with trains of n bits. The average probability of error for each train bit over this ensemble is one-half, regardless of the level of random noise or interference. We now derive the ensemble average probability of word error.

Consider an enciphered word of k bits. The probability of a word error, P_{cw}, is defined to be the probability of one or more erroneous bits. The probability of a word error and a train of external origin extending into the word is denoted by $P(w,t)$. If no train of external origin extends into the word, the probability of word error is denoted by $P(w|\overline{t})$. The probability that a train of external origin does not extend into a word is denoted by $P(\overline{t})$. It then follows from the theorem of total probability that

$$P_{cw} = P(w,t) + P(w|\overline{t})\ P(\overline{t}). \tag{9}$$

A train will extend into a word if, and only if, one of the $n-1$ bits immediately preceding the word is in error due to random noise. Thus assuming bit errors are uncorrelated,

$$P(\bar{t}) = (1 - P_b)^{n-1}. \tag{10}$$

Clearly, $P(w|\bar{t})$ is the same as the probability of a word error for plain text. From Eq. (2) we obtain

$$P(w|\bar{t}) = 1 - (1 - P_b)^k. \tag{11}$$

To determine $P(w, t)$, additional notation must be introduced. If i bits of a train of external origin extend into a word, we denote this condition by the symbols $tb = i$. For example, $P(tb = i)$ denotes the probability that a word contains i externally generated train bits. Since $P(w, t|tb = i) = P(w|tb = i)$, we can write

$$\begin{aligned} P(w, t) &= P(w|tb = k)\, P(tb = k) \\ &+ \sum_{i=1}^{k-1} P(w|tb = i)\, P(tb = i). \end{aligned} \tag{12}$$

If at least one of the $n-k$ bits preceding the word is in error and $n > k$, it is clear that $tb = k$. Thus

$$P(tb = k) = \begin{cases} 1 - (1 - P_b)^{n-k}, & n > k; \\ 0, & n \leqslant k. \end{cases} \tag{13}$$

For $tb = i$, where $1 \leqslant i < k$, it is necessary that there be an error precisely $n - i$ bits prior to the word but no erroneous bits among the next $n - i - 1$ bits. Therefore, for $1 \leqslant i < k$,

$$P(tb = i) = \begin{cases} P_b\,(1 - P_b)^{n-i-1}, & n > i; \\ 0, & n \leqslant i. \end{cases} \tag{14}$$

Substitution of Eqs. (10) through (14) into Eq. (9) yields

$$\begin{aligned} P_{cw} &= P(w|tb = k)\left[1 - (1 - P_b)^{n-k}\right] u(n-k) \\ &+ \sum_{i=1}^{\min(k-1,n-1)} P(w|tb = i)\, P_b(1 - P_b)^{n-i-1} + \left[1 - (1 - P_b)^k\right](1 - P_b)^{n-1}, \end{aligned} \tag{15}$$

where $u(n-k)$ is a step function, i.e., $u(n-k)$ is zero for $n \leqslant k$ and is one for $n > k$. Note that in the summation term, i extends to the least of the two integers $k-1$ and $n-1$. To reduce Fq. (15) further, we would have to know the exact configuration of the cryptographic system, since $P(w|tb = k)$ and the $P(w|tb = i)$ depend on the interaction of train

bits. As mentioned previously, it is more relevant to derive the average of P_{cw} over the ensemble of all possible cryptographic systems characterized by a specific value of the parameter n.

The ensemble average probability of bit error is one-half for every bit in a train, regardless of interference level.

Let a bar over the P indicate an ensemble average. To determine $\overline{P}(w|tb = i)$, note that when $tb = i$ there are i bits with an ensemble average probability of error equal to one-half. For no word error to occur, each of these i bits must be correct and each of the word bits at the input of the deciphering system must be correct, for if a word bit is in error at the input, it will trigger an internal train. It follows that

$$\overline{P}(w|tb = i) = 1 - \left(\frac{1}{2}\right)^i (1 - P_b)^k. \tag{16}$$

Similarly

$$\overline{P}(w|tb = k) = 1 - \left(\frac{1}{2}\right)^k (1 - P_b)^k. \tag{17}$$

From Eqs. (15) through (17), we obtain

$$\begin{aligned}\overline{P}_{cw} = {} & [1 - 2^{-k}(1 - P_b)^k]\,[1 - (1 - P_b)^{n-k}]\,u(n - k) \\ & + \sum^{\min(k-1,n-1)} P_b\,(1 - P_b)^{n-i-1}[1 - 2^{-i}(1 - P_b)^k] \\ & + [1 - (1 - P_b)^k]\,(1 - P_b)^{n-1},\end{aligned} \tag{18}$$

which can be put in the form of Eq. (4).

Equation (18) is the formula for the general cryptographic word error rate. To obtain the cryptographic bit error rate, set $k = 1$ in Eq. (18); this yields

$$\overline{P}_{cb} = \frac{1}{2}(1 + P_b)\left[1 - (1 - P_b)^{n-1}\right] + P_b(1 - P_b)^{n-1}. \tag{19}$$

Approximations to the formulas can be obtained by employing Maclaurin series expansion about the point $P_b = 0$. By this technique the plain-text word error rate given by Eq. (2) can be shown to be approximately

$$P_w \approx kP_b \tag{20}$$

under the condition that

$$P_b \ll \frac{2}{k - 1}, \qquad k > 1. \tag{21}$$

By the same method, Eq. (19) becomes

$$\overline{P}_{cb} \approx \left(\frac{n+1}{2}\right) P_b \tag{22}$$

under the condition that

$$P_b \ll \frac{2n+1}{n(n-1)}, \qquad n > 1. \tag{23}$$

A Maclaurin-series expansion of Eq. (18) yields

$$\overline{P}_{cw} = \begin{cases} [n + k - 2 - 2^{-k}(n - k - 2)]\, P_b, & n > k; \\ [n + k - 2 + 2^{-(n-1)}]\, P_b, & n \leq k. \end{cases} \tag{24}$$

The condition of validity obtained by this procedure is too complicated to be useful. Thus we derive Eq. (24) by an alternative technique which yields a simple condition of validity. First, each of the terms of the form $(1 - P_b)^m$ is expanded separately, dropping quadratic and higher order terms. Substitution into Eq. (18) yields an approximate expression for $\overline{P}_{cw}$ that still contains quadratic terms in P_b. If these terms are dropped, we are left with Eq. (24). The various conditions arising from each step of this procedure can be combined into a single condition of validity:

$$P_b \ll \min\left\{(n-1)^{-1}, k^{-1}\right\}. \tag{25}$$

This condition is more restrictive than those given in Eqs. (21) and (23). Thus Eq. (25) is a sufficient condition for the validity of Eqs. (20), (22), and (24). A slightly more convenient and more restrictive sufficient condition is given by Eq. (8).

AN EXAMPLE: PSK MODULATION

In this section it is assumed that the information is transmitted by means of phase shift keying (PSK). If white Gaussian noise is present at the receiver input, the plain-text bit error rate for an ideal receiver is given by (5)

$$P_b = \operatorname{erfc}\left(\sqrt{\frac{2E_b}{N_0}}\right), \tag{26}$$

where by definition

$$\operatorname{erfc}(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty \exp\left(-\frac{x^2}{2}\right) dx. \tag{27}$$

Note that Eq. (26) is in the form of Eq. (1).

In this example we let $n = 60$ and $k = 10$. Application of Eqs. (2), (3), (4a), and (26) leads to the plots shown in Fig. 3. Alternatively, according to Eq. (8), we could use Eqs. (5), (6), (7), and (26) to determine the points where $P_b < 10^{-4}$.

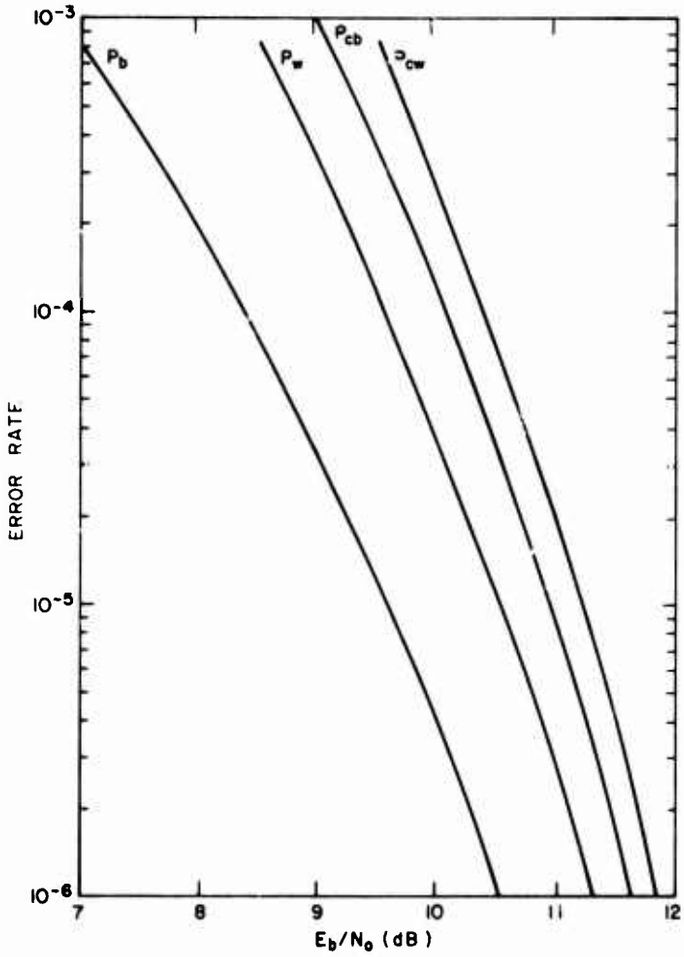

Fig. 3 — Bit and word error rates

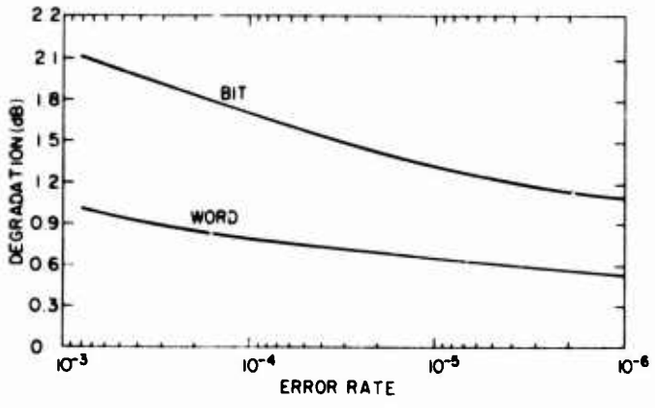

Fig. 4 — Degradation as a function of plain-text error rate

From Fig. 3 the degradation due to the enciphering can be determined. In Fig. 4 the degradation for a cryptographic bit is plotted as a function of the plain-text bit error rate. In the same figure the corresponding curve for a 10-bit cryptographic word is plotted as a function of the plain-text word error rate.

Suppose 10-bit words are to be transmitted at a word error rate of 10^{-5}. According to Fig. 4, an additional 0.7 dB of power is required, when enciphering is employed, to maintain the error rate. Assuming this power is provided, is the performance of the cryptographic system as good as the plain-text system? The answer is usually no, due to the different costs of word errors in these systems. A word error in a plain-text system usually involves a single erroneous bit. On the other hand, in a cryptographic system a word error usually implies several erroneous bits. Thus the cryptographic word error causes a more severe misinterpretation of the transmitted data.

It is seen in Fig. 4 that for a cryptographic system, approximately 1.3 dB of extra power are required to maintain a bit error rate of 10^{-5}. Again the question arises as to the relative performance of the cryptographic and plain-text systems. In this case the performances are usually comparable. In the cryptographic system the bit errors occur in clusters. Thus although there are fewer word errors than in the plain-text system, the bit errors do greater damage. Relative performance must be determined by weighing the costs of a word error with a single erroneous bit relative to those of a word error with several bit errors.

CORRELATED BIT ERRORS

So far it has been assumed that at the input to the deciphering system bit errors occur independently of each other. There are many important situations in which this assumption is untenable. In this section an example is presented which indicates how the theory can be extended to handle correlated bit errors.

It is sometimes desirable to encode cryptographic or plain bits in terms of bit transitions. For example, after encoding a ZERO may be represented by a transition; a ONE may be represented by no transition. With this representation, the transmitted signal can be inverted in polarity without affecting its interpretation. This representation is called differential encoding. It is useful in phase-locked-loop systems and other systems which have no sense of absolute polarity. The original bits can be recovered by sampling the differentially encoded bits and comparing the polarity of adjacent samples to determine if a transition has occurred. Figure 5 illustrates a cryptographic system with differential detection. We now proceed to determine the word and bit error rates at the output of the deciphering system.

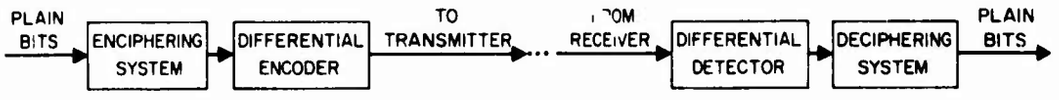

Fig. 5 — Cryptographic system with differential detector

The calculation of the word error rate is a straightforward but extremely tedious extension of the method used for the uncorrelated bit error case. The reason for the complexity will now be explained. Consider two consecutive bits at the input of the differential detector. Since the detector compares the polarity of adjacent bits, bit errors will usually occur in pairs. The exception is when the two consecutive bits are both in error. Then the second bit at the output of the detector will be correct, since the relative state of the second input bit is unchanged with respect to the first input bit. Taking the latter situation into account is what makes the analysis difficult. If P_b is small, as is normally true in practical

systems, we can obtain accurate asymptotic formulas by ignoring the latter anomaly. Thus we assume that a bit error at the input of the differential detector will always cause two consecutive erroneous bits at the output of the detector.

Under the latter assumption the trains will be $n + 1$ bits long. Clearly, Eq. (11) will remain the same as in the previous derivation. Equations (10) and (13) must be modified by substituting $n + 1$ for the symbol n in these relations. However, Eq. (14) is altered in a different manner. The reason is that for $tb = i$, where $1 \leqslant i < k$, it is necessary that there be an error at the input to the detector precisely $n - i + 1$ bits prior to the word. The bit located exactly $n - i$ bits prior to the word is then automatically erroneous at the detector output, according to our assumption. It is, however, necessary that there be no errors among the $n - i - 1$ bits preceding the word at the input to the detector. From these considerations, we have

$$P(tb = i) = \begin{cases} P_b\,(1 - P_b)^{n-i-1}, & n > i; \\ P_b, & n = i; \\ 0, & n < i. \end{cases} \tag{28}$$

Similar reasoning shows that Eqs. (16) and (17) remain unchanged except when $tb = n$. In this case, $\overline{P}(w|tb = n) = 1$ because of the initial assumption.

Using the same methods previously employed and some algebraic manipulation, it follows that the asymptotic formulas for word and bit error rates of the system of Fig. 5 are

$$\overline{P}_{cw} = \begin{cases} [n + k - 1 - 2^{-k}\,(n - k - 1)]\,P_b, & n > k; \\ [n + k - 1 - 2^{-(n-1)}]\,P_b, & n \leqslant k. \end{cases} \tag{29}$$

$$\overline{P}_{cb} = \begin{cases} \left(\frac{n + 2}{2}\right) P_b, & n > 1; \\ 2P_b, & n = 1. \end{cases} \tag{30}$$

Equations (29) and (30) could not have been obtained directly by substituting $n + 1$ for the symbol n in Eqs. (22) and (24). When $n = 1$, it is seen that $\overline{P}_{cb} = 2P_b$, which is a restatement of our initial assumption concerning the operation of the differential detector. A sufficient condition for the validity of Eqs. (29) and (30) can be given once again by Eq. (8).

In the previous example of PSK modulation with $n = 60$ and $k = 10$, it is seen that the differential encoding causes utterly negligible degradation for small values of P_b.

REFERENCES

1. T. Twigg, Electronic Design 23, 68 (1972).

2. C.H. Meyer and W.L. Tuchman, Electronic Design 23, 74 (1972).

3. S.W. Golomb, *Shift Register Sequences*, Holden-Day, San Francisco, 1967.

4. A. Sinkov, *Elementary Cryptanalysis, A Mathematical Approach*, Random House, New York, 1968.

5. H.L. Van Trees, *Detection, Estimation, and Modulation Theory*, Part I, Wiley, New York, 1968.